THEORIA

DE

CONGRUENTIAS INTRA NUMEROS INTEGRO

PER

MICHAELE CIPOLLA

Congruentias in genere - Theorema de Fermat, de Eulero et de Wilson - Congruentias de primo gradu - Congruentias de secundo gradu - Congruentias binomio - Gaussiano, radices primitivo, indices - Applicationes.

CORILEONE, januario-aprile 1904.

THEORIA

de

CONGRUENTIAS INTRA NUMEROS INTEGRO

per

MICHAELE CIPOLLA

Congruentias in genere - Theorema de Fermat, de Eulero et de Wilson - Congruentias de primo gradu - Congruentias de secundo gradu - Congruentias binomio - Gaussiano, radices primitivo, indices - Applicationes.

In ce scripto me collige, in ordine de tractatione, propositiones de theoria de congruentias intra numeros integro, que constitue primo parte de theoria de numeros que me spera confice postea.

Me adde et aliquo notitia historico et bibliographico, ut que lege pote cognosce origine et progressu de theoria et adhibe operas que contine suo explicatione.

Me non arroga ad me ut asseque proposito omnino in perfecto modo, sed me spera reverte ad incepto ut commuta et corrige, et adpone additamento sive in propositiones sive in notitia historico et bibliographico. Ideo me pete benevolentia et favore de omni que excole et dilige tali parte de Analysi, que cum optimo iure Gauss appella regina de Mathematica et me es laeto recipe consilio de omni genere.

Operas
que tracta de theoria de congruentias

A. M. Legendre, *Essai sur la théorie des nombres*. Paris 1e éd. an VI (1798); 2e éd. 1808; 3e éd. 1830; réimpression facsimile de la troisième éd, Paris: Hermann, 1899 — Traductio in lingua germanico per H. Maser ex 3 ed., Leipzig 1886; ex 2 ed. Leipzig 1893.

C. F. Gauss, *Disquisitiones arithmeticae*, Lipsiae, 1801 (= = Werke t. I) — Traductione in franco de Poullet-Delisle

(Recherches arithmétiques, Paris, 1807) — Traductione in lingua germanico de H. MASER *(Untesuchungen über hohere Arithmetik*, Berlin, 1889).

L. POINSOT, *Réflexions sur les principes fondamentaux de la théorie des nombres*, Journal de Liouville, t. X, 1845.

P. L. TCHEBYCHEF, Theoria de congruentias (in russo), S. Petroburgo, 1847. — Traductione in lingua germanico per H. SCHAPIRA, Berlin 1889. — Traductione in italico per I. MASSARINI, Roma 1895.

V. A. LEBESGUE, *Exercices d'Analyse numérique*, Paris 1859; *Introduction à la Théorie des nombres*, Paris 1868.

H. I. ST. SMITH, *Report on the Theory of Numbers*, British Assoc. for the advancement of Sc., 1859, p. 228; 1860, p. 120; 1861, p. 292; 1863, p. 168; 1865, p. 322 = Coll. Math. Papers t. I., p. 38, 93, 163, 229, 263, 289.

P. LEJEUNE-DIRICHLET, *Vorlesungen über Zahlentheorie*, herausgegebenen von R. DEDEKIND, Braunschweig, 1 Auf. 1863, 2 Auf. 1871, 3 Auf. 1879, 4 Auf. 1894. — Traductione in italico ex 3 ed. per A. FAIFOFER, Venezia, 1881. — Traductione in russo, parte 1, per J. M. NASARJEWY, S. Petroburgo, 1899.

J. A. SERRET, *Cours d'Algèbre Superieure*, 4e éd., 2 v., Paris 1877, 5e éd., 1885.
— Traductione in lingua germanico per G. WERTHEIM, Leipzig 1878.

G. WERTHEIM, *Elemente der Zahlentheorie*, Leipzig, 1887.

J. SOCHOTZKY, Algebra Superiore, v. 2, Fundamenta de theoria de numeros (in russo), S. Petroburgo, 1888.

T. J. STIELTJES, *Sur la theorie des nombres. Etude bibliographique.* Ann. de Toulouse, IV, 1890, pp. 1-103; Paris, Gauthier-Villars, 1895.

E. LUCAS, *Théorie des Nombres*, t. I. Paris 1891. (Alio tomo non es publicato pro morte de auctore).

P. BACHMANN, *Die Elemente der Zahlentheorie*, Leipzig, 1892.

G. B. MATHEWS, *Theory of Numbers*, Part. I, Cambridge 1892.

U. SCARPIS, *Primi elementi della Teoria dei numeri*, Milano, Hoepli, 1897.

E. CAHEN, *Elements de la Théorie des nombres*, Paris. 1900.

P. BACHMANN, *Niedere Zahlentheorie*, Encykl. d. math. wiss. t. I, pp. 551-581. — I Teil, Leipzig, pp. X + 402, 1902.

L. KRONECKER, *Vorlesungen über Mathematik;* 2 Teil, *Vorlesungen über allgemeine Arithmetik*; hrsg. von K. HENSEL, 1 Absch., *Vorlesungen uber Zahlentheorie*, 1 Band, Leipzig, 1901.

G. WERTHEIM, *Onfangsgründe der Zahlenlehre*, Braunschweig, 1902.

P. GAZZANIGA, *Gli elementi della teoria dei numeri*, Padova, Frat. Drucker, 1903.

§ 1 Congruentias in genere

* 1. $m, n \varepsilon N_1 \,.\, a,b,c,d \varepsilon n \,.\supset:$

·1 $a \varepsilon\, b+mn \,.=.\, b \varepsilon\, a+mn \,.=.\, a-b \,\varepsilon mn$

GAUSS scribe relatione $a \varepsilon\, b+mn$ ita

$$a \equiv b \text{ (mod. } m)$$

et voca illo « congruentia » : « Si numerus *a* numerorum *b*, *c* differentiam metitur, *b* et *c* secundum *a congrui* dicuntur, sin minus, *incongrui:* ipsum *a modulum* appellamus. Uterque numerorum *b*, *c*, priori in casu alterius *residuum*, in posteriori vero *non residuum* vocatur » (D. A., art. 1.).

LEGENDRE scribe $a = b + M\,(m)$ et es contrario ad symbolo et denominatione de GAUSS : « Ces équations entre des restes... se traitent comme les équations ordinaires, sans qu'il soit besoin des signes nouveaux d'égalité ni des dénominations nouvelles assez *incongrues*, dont quelques géomètres font usage ». (*Essai*, etc., 2e éd., 2e suppl., p. 12, note).

CATALAN seque notatione de LEGENDRE: « Admirables (les Recherches Arithmétiques de Gauss) sauf les dénominations et la notation. POULLET-DELISLE, traducteur de Gauss, dit qu' *elles peuvent étonner*. De son côté, LEGENDRE s'est raillé des *espressions incongrues*, adoptées par le Géometre de Brunswick. Mais LEGENDRE et DELISLE avaient des oreilles françaises » (v. *Mélanges mathématiques* par E. C. CATALAN, in Mémoires de la Société Royale des Sciences de Liège, t. XIII, s. 2, 1886, p. 334).

Hodie denominatione et symbolo de GAUSS es communi ad maximo parte de auctore, sed non es necessario introduc novo

symbolo in ce scripto, quod notatione $a \varepsilon\ b + m\mathrm{n}$ es satis simplice.

·2 $a \varepsilon\ b + m\mathrm{n} \,.\, b \varepsilon\ c + m\mathrm{n} \,.\supset.\, a \varepsilon\ c + m\mathrm{n}$

·3 $\text{———} \,.\supset.\, a + c\ \varepsilon\ b + c + m\mathrm{n}$

·31 $\text{———} \,.\supset.\, a - c\ \varepsilon\ b - c + m\mathrm{n}$

·4 $\text{———} \,.\, c \varepsilon\ d + m\mathrm{n} \,.\supset.\, a + c\ \varepsilon\ b + d + m\mathrm{n}$

·41 $\text{——————} \,.\supset.\, a - c\ \varepsilon\ b - d + m\mathrm{n}$

·5 $\text{———} \,.\supset.\, ac\ \varepsilon\ bc + m\mathrm{n}$

·51 $\text{———} \,.\, c \varepsilon\ d + m\mathrm{n} \,.\supset.\, ac\ \varepsilon\ bd + m\mathrm{n}$

·52 $\text{———} \,.\, r \varepsilon \mathrm{N}_0 \,.\supset.\, a^r\ \varepsilon\ b^r + m\mathrm{n}$

·6 $ac\ \varepsilon\ bc + m\mathrm{n} \,.\supset.\, a\ \varepsilon\ b + [m/\mathrm{D}(c,m)]\mathrm{n}$

·7 $(b + m\mathrm{n}) \frown (b + n\mathrm{n}) = b + \mathrm{mlt}(m,n) \times \mathrm{n}$

·8 $a \,-\varepsilon\ b + \mathrm{nD}(m,n) \,.\supset.\, -\exists\ (a + m\mathrm{n}) \frown (b + n\mathrm{n})$

·9 $a \varepsilon\ b + \mathrm{nD}(m,n) \,.\supset.\, (a + \mathrm{n}m) \frown (b + \mathrm{n}n) =$
$a + m\{\mathrm{n} \frown x \ni [mx/\mathrm{D}(m,n)\ \varepsilon\ (b - a)/\mathrm{D}(m,n) + \mathrm{n}n/\mathrm{D}(m,n)]\}$

·91 $\mathrm{D}(m,n) = 1 \,.\supset.\, (a + \mathrm{n}m) \frown (b + \mathrm{n}n) = a + \mathrm{n}m \frown (b - a + \mathrm{n}n)$

§ 2 **Residuo de functiones particulari**

***** 2. $p \varepsilon \mathrm{Np} \,.\, m,n \varepsilon\ \mathrm{N}_1 \,.\supset:$

·1 $\mathrm{C}(m,n)\ \varepsilon\ \mathrm{C}[\mathrm{quot}(m,p),\ \mathrm{quot}(n,p)] \times$
$\times \mathrm{C}[\mathrm{rest}(m,p), \mathrm{rest}(n,p)] + p\mathrm{n}$

·2 $\mathrm{C}(m,n)\ \varepsilon\ \Pi[\mathrm{C}\{\mathrm{rest}[\mathrm{quot}(m,p^r)], \mathrm{rest}[\mathrm{quot}(n,p^r),p]\} | r, \mathrm{N}_0] + \mathrm{n}p$

·21 $m,n\ \varepsilon\ \mathrm{n}p \,.\supset.\, \mathrm{C}(m,n)\ \varepsilon\ \mathrm{C}[\mathrm{quot}(m,p),\ \mathrm{quot}(n,p)] + \mathrm{n}p$

·22 $n \varepsilon\ 1 \cdots (p - 1) \,.\supset.\, \mathrm{C}(p,n)\ \varepsilon\ \mathrm{N}_1 \times p$

{LEIBNIZ, Math. Schr., t.7, p.102}

·23 $n \varepsilon\ 0 \cdots (p - 1) \,.\supset.\, \mathrm{C}(p - 1, n)\ \varepsilon\ (-1)^n + \mathrm{N}_0 \times p$

·24 $n \varepsilon\ 0 \cdots (p - 2) \,.\supset.\, \mathrm{C}(p - 2, n)\ \varepsilon\ (-1)^n (n + 1) + \mathrm{N}_0 \times p$

·25 $n \varepsilon 0 \cdots (p-3) . \supset . C(p-3,n) \; \varepsilon \; (-1)^n (n+1)(n+2)/2 + N_0 \times p$

·26 $p \varepsilon \mathrm{Np} - \iota 2 . n \varepsilon 2 \cdots (p-1) . \supset . C(p+1,n) \; \varepsilon \; N_1 \times p$

{2·1·2···26, LUCAS, American J. a. 1878, t. I. p. 229, et Théorie des nombres, 1891, pp. 417-420}

P2·22 = Form. 1902, p. 72, 12·7 . ·23 = F, p. 72, 12·71 . ·24 = F, p. 72, 12·73 . ·26 = F, p. 72, 12·72.

✻ 3. $p \varepsilon \mathrm{Np} . m \varepsilon N_1 . \supset :$

·1 $m - \varepsilon (p-1) \times N_0 . \supset . \Sigma[1 \cdots (p-1)]^m \; \varepsilon \; N_1 \times p$

{LIONNET, v. CATALAN, Mém. de l'Ac. de Belgique, t. 46, 1886, p. 14}

·2 $m \varepsilon (p-1) \times N_0 . \supset . \Sigma[1 \cdots (p-1)]^m \; \varepsilon \; -1 + N_1 \times p$

·3 $p \varepsilon \mathrm{Np} . p > 3 . \supset . \mathrm{nt}\Sigma/[1 \cdots (p-1)] \; \varepsilon \; p^2 \times N_1$

{OSBORN, 1892, The Messenger of Math., t. 22, p. 51}

·4 $p \varepsilon \mathrm{Np} . p > 3 . \supset . \mathrm{nt}\Sigma/[1 \cdots (p-1)]^2 \; \varepsilon \; p \times N_1$

{GLAISHER, 1900, Quarterly Journ. of Math. t. 31, p. 337}

P3·1 = F, p. 138, 20·1 . ·3 = F, p. 138, 20·1 . ·4 = F, p. 138, 20·2.

§ 3 Theorema de Fermat, de Eulero et de Wilson

✻ 4. $m \varepsilon N_1 . p \varepsilon \mathrm{Np} . a \varepsilon \mathrm{n} . \supset :$

·1 $D(a,m) = 1 . \supset . a \curlywedge \Phi m \; \varepsilon \; 1 + m\mathrm{n}$

Ce propositione es dicto « theorema de EULERO », nam illo pertine ad EULERO, que primo stude functione Φ (EULER, Novi Comm. Acad. Sc. Petrop. a. 1760-61, t. 8, pp. 85-103, Act. Ac. Sc. Petrop. a. 1780, t. 4_2, p. 18; Φm = numero de numeros que non supera m et es primo cum m). Symbolo Φ es introducto a GAUSS (1801, Werke t. 1 p. 30); EULERO ute simbolo Π (Acta Ac. Sc. Petrop., 1780, p. 18). LUCAS (T. de Nombres, 1891) voca illo *indicatore*, vocabulo introducto a CAUCHY (Oeuvres, s. 1, t. 6, p. 124) in sensu pauco differente).

·11 $a - \varepsilon \mathrm{n}p . \supset . a^{p-1} \; \varepsilon \; 1 + \mathrm{n}p$

Ce theorema maxime elegante et fondamentali in theoria de congruentias es appellato *theorema de Fermat*, quod FERMAT

primo (a. 1640) enuntia illo (v. Oeuvres, Paris 1891, t.2 p. 209). LEIBNIZ primo demonstra illo (Math. Schr. t. 7, p. 154), sed suo demonstratione non es noto in tempore de GAUSS (v. D. A., p. 54 nota).

EULERO publica primo demonstratione in Comm. Ac. Sc. Petrop., t. 8, p. 143 (a. 1736), et altero in Novi Comm. Ac. Sc. Petrop., t. 8, p. 70. Vide et LAMBERT, Acta Eruditorum, a. 1769, p. 109; Gauss, D. A. art. 49-51; LEGENDRE, Essai etc, 2e éd., n. 129.

Secundum HEANS (Messenger of Math., a. 1898, t. 27, p. 174), Mathematicos sinense novi ce theorema, per $a=2$, e tempore de CONFUCIO (CON-FU-TSE) a. —550 ⊢ —447; sed illos puta es vero propositione inverso:

$$p \varepsilon \mathrm{N}_1 \,.\, 2^p - 2 \;\varepsilon\; \mathrm{N}_1 \times p \;.\supset.\; p \varepsilon \mathrm{N}p,$$

quod es falso (v. meo scripto: Sui numeri composti che verificano la congruenza di Fermat $a^{P-1} \equiv 1$ (mod. P), Ann. di Mat, a. 1903, t. 9, s. 3, pp. 139-160; v. et P 49, 50 de ce scripto).

·2 $m \varepsilon (\mathrm{N}_1 + 4) - \mathrm{N}p \;.\supset.\; (m-2)! \;\varepsilon\; \mathrm{N}_1 m$

·3 $(p-2)! \;\varepsilon\; 1 + \mathrm{N}_0 \times p$

}2·3 LEIBNIZ, Mss. Mat. t.3 B11 fol. 10

·4 $(p-1)! \;\varepsilon\; -1 + \mathrm{N}_1 \times p$

Ce propositione es dicto «theorema de WILSON», quod WARING, (*Meditationes Algebricae* ed. I., a. 1770, p. 218; ed. III, a. 1782, p. 382), attribue illo ad WILSON, suo discipulo. Primo demonstratione de ce P. pertine ad LAGRANGE (Nouv. Mém de l'Ac. de Berlin, a. 1771, t. 2, p. 125 = Oeuvres, t. 3, p. 425). EULERO trade novo demonstratione in *Opuscula analytica*, S. Petr. a. 1783, t. 1., p. 329), GAUSS alio in Disquis. arith., art. 77 et alio LEGENDRE in Essai, 2e ed. n. 130.

Theorema de WILSON es casu particulari de propositione circa numeros primo que pertine ad J. STEINER (J. f. Math. t. 13, a. 1835, p. 356 = Werke t. 2, p.7: vide et JACOBI, ibidem t. 14, a. 1835, p. 64 = Werke t. 6, p. 262).

·5 $p \varepsilon \mathrm{N}p \;.=.\; p \varepsilon \mathrm{N}_1 + 1 \,.\, (p-1)! + 1 \;\varepsilon\; \mathrm{N}_1 \times p$

·6 $p \;\varepsilon\; 4\mathrm{N}_1 + 1 \;.\supset.\; \{[(p-1)/2]!\}^2 \;\varepsilon\; -1 + \mathrm{N}_1 \times p$

·7 $p \varepsilon 4N_1-1 .\supset. \{[(p+1)/2]!\}^2 \varepsilon 1+N_1 \times p$

(P ·6 ·7 es enuntiato in *Meditationes algebricae de* WARING (a. 1770) sed demostratione pertine ad LAGRANGE (a. 1771, Oeuvres, t. 3, p. 431) Vide et LEGENDRE, Essai, 2[e] éd, n. 131.:

P ·7 pote es enuntiato

$p\varepsilon 4N_1-1 .\supset. [(p+1)/2]! \varepsilon (1+N_1 \times p) \cup (-1+N_1 \times p)$

Quaestione de investiga in quali casu residuo de $[(p+1)/2]!$, sequente modulo p, es congruo 1 aut —1, posito a LEJEUNE-DIRICHLET (J. f. Math., t. 3, a 1828, p. 401 = Werke t. 1, p. 105) es resoluto a JACOBI (ibidem, t. 9, 1832, p. 189 = Werke t. 6, p. 240), que trade ce propositione

$p\varepsilon 4N_1-1 .\supset. [(p+1)/2]! \varepsilon (-1) \uparrow \text{Num}[(p+1)/2 \cdots p \frown n^2+np]$

KRONECKER et LIOUVILLE da alio regulas minus simplice [J. de Math (2), t. 5, 1860, p. 127, 267]

·8 $m\varepsilon (\text{Np}-\iota 2)\uparrow N_1 \cup 2[(\text{Np}-\iota 2)\uparrow N_1] \cup \iota 4 .\supset.$
$\Pi\{1 \cdots m \frown x \ni [D(x,m)=1]\} \varepsilon -1+N_1 m$

·9 $m\varepsilon N_1 - \iota 4 - (\text{Np}-\iota 2)\uparrow N_1 - 2[(\text{Np}-\iota 2)\uparrow N_1] .\supset.$
$\Pi\{1 \cdots m \frown x \varepsilon [D(x,m)=1]\} \varepsilon 1+N_0 m$

P ·8 ·9 constitue « theorema de WILSON amplificato ». GAUSS (D. A. art. 70) enuntia illo et da aliquo notione circa demonstratione, pro que vide BRENNECKE, CRELLE et ARNDT, J. f. Math., t. 19, a. 1839, p. 319; t. 20, a. 1840, p. 29, et t. 31, a. 1846, p. 329.

P4·1 F. 1902, p. 143, P·2 . ·11 F. p. 71, P·2. . P4·2 F. p. 72, 12·1 . ·3 F. p. 72, 12·2 . ·4 F. 12·3 . ·5 F. 12·4 . ·6 F. 12·5 . ·7 F. 12·6.

✻ 5.

·0 $m\varepsilon N_1+1 - 8N_1 .\supset. \Psi m = \text{mlt}[\Phi x | x, (\text{Np}\uparrow N_1) \frown m/N_1]$ Df

·01 $m\varepsilon 8N_1 . n\varepsilon \text{mp}(2,m) .\supset.$
$\Psi m = \text{mlt}\{2^{n-2}, \Phi x | x, [(\text{Np}-\iota 2)\uparrow N_1] \frown m/N_1\}$ Df

·02 $\Psi 1 = 1$ Df

·1 $m\varepsilon N_1 .\supset. \Psi m \varepsilon N_1 \frown m/N_1$

·2 $m\varepsilon N_1 - \iota 4 - (\text{Np}-\iota 2) - 2[(\text{Np}-\iota 2)\uparrow N_1] .\supset. \Psi m < \Phi m$

Ψm = indicatore reducto de m, v. LUCAS, Théorie des Nombres, 1891, p. 428

·3 $p\varepsilon \text{Np}-\iota 2 . a,b\varepsilon n-np . r,s\varepsilon N_1 . a\varepsilon b+p_r(n-np) .\supset.$
$a\uparrow p^s \varepsilon b\uparrow p^s + p^{r+s}(n-np)$

$\cdot 31$ $a,b \varepsilon 2\mathrm{n}+1 \,.\, r,s \varepsilon \mathrm{N}_1+1 \,.\, a \varepsilon b+2^r(2\mathrm{n}+1) \,.\supset.$
$a^s \varepsilon b^s+2^{r+s}(2\mathrm{n}+1)$

$\cdot 32$ $a \varepsilon 2\mathrm{n}+1 \,.\, s \varepsilon \mathrm{N}_1+2 \,.\supset.\, a \uparrow 2^{s-2} \varepsilon 1+2^s\mathrm{n}$
(V. GAUSS, Disq. Arith. art. 90.)

$\cdot 4$ $a \varepsilon \mathrm{n} \,.\, m \varepsilon \mathrm{N}_1 \,.\, \mathrm{D}(a,m)=1 \,.\supset.\, a \uparrow \Psi m \varepsilon 1+\mathrm{n}m$

$\cdot 5$ $a \varepsilon \mathrm{n} \,.\, m \varepsilon \mathrm{N}_1 \,.\, n= \max[\mathrm{mp}(x,a)|x,\mathrm{Np}] \,.\supset.$
$a \uparrow (n+\Psi m) \varepsilon a \uparrow n+ m\mathrm{n}$
(LUCAS, Th. d. N., p. 430)

§ 4 Congruentias de primo gradu

✻ 6. $a,b \varepsilon \mathrm{n} \,.\, m \varepsilon \mathrm{N}_1 \,.\supset:$

$\cdot 1$ $b \varepsilon \mathrm{n} - \mathrm{n}\mathrm{D}(a,m) \,.\supset.\, -\exists\, \mathrm{n} \frown x \ni (ax+b \varepsilon m\mathrm{n})$

$\cdot 2$ $b \varepsilon \mathrm{n}\mathrm{D}(a,m) \,.\supset.\, \mathrm{n} \frown x \ni (ax+b \varepsilon \mathrm{n}m) =$
$\mathrm{n} \frown x \ni [(ax+b)/\mathrm{D}(a,m) \varepsilon \mathrm{n}m/\mathrm{D}(a,m)]$

$\cdot 3$ $b \varepsilon \mathrm{n}\mathrm{D}(a,m) \,.\supset.\, \mathrm{Num}[o \cdots (m-1) \frown x \ni (ax+b \varepsilon m\mathrm{n})] = \mathrm{D}(a,m)$

$\cdot 4$ $\mathrm{D}(a,m)=1 \,.\supset.\, \mathrm{n} \frown x \ni (ax+b \varepsilon m\mathrm{n}) = -ba \uparrow (\Psi m-1)+m\mathrm{n}$

$\cdot 41$ $p \varepsilon \mathrm{Np} \,.\, \mathrm{D}(a,p) =1 \,.\supset.\, \mathrm{n} \frown x \ni (ax+b \varepsilon \mathrm{n}p) = -ba^{p-2}+m\mathrm{n}$

In ce propositiones es methodo ut investiga solutione de congruentia de primo gradu. Secundum P ·4·41 metodo trahe origine ex theorema de Fermat (4·11) et de Eulero (4·1) aut ex propositione 5·4. Congruentia de primo gradu pote es resoluto cum methodo ut resolve aequatione indeterminato de primo grado, p. ex. cum auxilio de fractione continuo, ut fac LAGRANGE (Histoire de l'Ac. de Berlin, a. 1767, p. 175). Vide et GAUSS, Disq. Arith., art. 26-31, LEGENDRE, Essai, 2e éd., § 11.

GAUSS (Disq. Arith., art. 31) scribe numeros que satisfac ad relatione $ax \varepsilon b+m\mathrm{n}$ sub forma $\frac{b}{a}$ (mod m). Ce expressione habe aut nullo aut uno aut plure valore incongruo (mod p). Hodie maximo parte de auctore non ute ce notatione de GAUSS.

❋ 7. $n \varepsilon \mathrm{N}_1 \,.\, m \varepsilon \mathrm{N}_1\mathrm{F}1\cdots n \,.\, a \varepsilon (\mathrm{n}-\iota 0)\mathrm{F}1\cdots n \,.\supset:$

·1 $r,s \,\varepsilon\, 1\cdots n \,.\, r<s \,.\supset_{r,s}.\, \mathrm{D}(m_r,m_s)=1 \,:\, u= \Pi(m,|1\cdots n) \,.$
$k \varepsilon\, \mathrm{nF}1\cdots n \,:r\varepsilon 1\cdots n.\supset_r.k_r \varepsilon\, \mathrm{n}\frown x\varepsilon(xu/a_r \,\varepsilon\, 1+m_r\mathrm{n}) \,:\supset:$
$\mathrm{n}\frown x\ni(r\varepsilon\, 1\cdots n \,.\supset_r.\, x\varepsilon\, a_r+\mathrm{n}m_r) = \Sigma(a_r k_r u/m_r|r,1\cdots n)+\mathrm{n}u$

·2 $\exists\, \mathrm{n}\frown x\ni(r\varepsilon\, 1\cdots n \,.\supset_r.\, x\varepsilon\, a_r+m_r\mathrm{n}) \,.=:\, r,s\varepsilon 1\cdots n \,.\supset_{r,s}.$
$a_r - a_s \,\varepsilon\, \mathrm{nD}(m_r,m_s)$

·3 $n_1 = \Pi\{x\upharpoonright \mathrm{mp}(x,m_1)|x,\, \mathrm{Np}\frown x\ni[r\varepsilon\, 2\cdots n \,.\supset_r.\mathrm{mp}(x,m_1) \geqq$
$\mathrm{mp}(x,a_r)] \,.\, r\varepsilon\, 2\cdots n \,.\, n_r = \Pi\{x\upharpoonright \mathrm{mp}(x,m_r)|x,\mathrm{Np}\frown x\ni[s\varepsilon\, 1\cdots n - \iota r \,.\supset_s.$
$\mathrm{mp}(x,m_r) > \mathrm{mp}(x,a_s)] \,.\supset:\, r,s\varepsilon\, 1\cdots n \,.\, r<s \,.\supset.\, \mathrm{D}(n_r,n_s)=1 \,.$
$\Pi(n_r|r,\, 1\cdots n) = \mathrm{mlt}(a_r|r,1\cdots n)$

·4 $\mathrm{Hp}\cdot2\cdot3 \,.\supset.\, \mathrm{n}\frown x\ni(r\varepsilon\, 1\cdots n \,.\supset_r.\, x\varepsilon\, a_r+\mathrm{n}m_r) =$
$= \mathrm{n}\frown x\ni(r\varepsilon 1\cdots n \,.\supset_r.\, x\varepsilon\, a_r+\mathrm{n}n_r)$

Ce propositiones, que constitue regulas de GAUSS (Disq. Arith. art. 32-36), es in antiquo libro de arithmetica de sinense Sun Tsze; v. K. D. BIERNATZKI, J. f. Math., t. 52, a. 1856, p. 59; MATTHIESSEN, ibidem, t. 91, 1881, p. 254. STIELTJES (Ann. de Toulouse, t. 4, 1890) tracta ce quaestione cum maximo claritate.

§ 5 Congruentias de secundo gradu

❋ 8. $a,b,c\varepsilon\mathrm{n} \,.\, p\varepsilon\, \mathrm{Np}-\iota 2 \,.\, \mathrm{D}(a,p)=1 \,.\supset:$

·1 $\mathrm{n}\frown x\ni(ax^2+bx+c \,\varepsilon\, \mathrm{n}p) = \mathrm{n}\frown x\ni[\exists\, \mathrm{n}\frown z\ni(z^2 \,\varepsilon\, b^2-4ac+\mathrm{n}p).$
$2ax+b \,\varepsilon\, z+\mathrm{n}p]$

{GAUSS, *Disqu. Arith.* art. 152}

·2 $a\upharpoonright[(p-1)/2] \,\varepsilon\, -1+\mathrm{n}p \,.\supset.\, -\exists\, \mathrm{n}\frown x\ni(x^2 \,\varepsilon\, a+\mathrm{n}p)$

·3 $a\upharpoonright[(p-1)/2] \,\varepsilon\, 1+\mathrm{n}p \,.\supset.\, \exists\, \mathrm{n}\frown x\ni(x^2 \,\varepsilon\, a+\mathrm{n}p)$

{·2·3 EULERO, *Opus. anal.* t. 1, a. 1773, p. 242, 268=*Comm. Arith. coll.* t. 2, p. 1, 13; GAUSS, *Disqu. Arith.* art. 106; LEGENDRE, *Essai*, 2e éd. n. 134}

·32 $a\upharpoonright[(p-1)/2]\varepsilon 1+\mathrm{n}p \,.\supset.\, \mathrm{Num}[1\cdots(p-1) \frown x\ni(x^2 \,\varepsilon\, a+\mathrm{n}p)]=2$

·32 ——————————— $.\, k\varepsilon\, 1\cdots(p-1) \frown x\ni(x^2 \,\varepsilon\, a+\mathrm{n}p) \,.\supset.$
$\iota k \cup \iota(p-k) = 1\cdots(p-1) \frown x\ni(x^2 \,\varepsilon\, a+\mathrm{n}p)$

❋ 9. $p,q \varepsilon \mathrm{Np}-\iota 2 \,.\, a,b \varepsilon \mathrm{n} \,.\supset:$

·0 $\mathrm{J}(a,p) = 1 \,.=.\, a \varepsilon (\mathrm{n}^2+\mathrm{n}p)-\mathrm{n}p$ Df

·01 $\mathrm{J}(a,p) = -1 \,.=.\, a -\varepsilon\, \mathrm{n}^2+\mathrm{n}p$ Df

·02 $\mathrm{J}(a,p) = 0 \,.=.\, a \varepsilon \mathrm{n}p$ Df

·03 $\mathrm{J}(a,p) \varepsilon [\iota 1 \cup \iota(-1) \cup \iota 0] \cap x \ni \{a \uparrow [(p-1)/2] \varepsilon x+\mathrm{n}p\}$ Dfp

{LEGENDRE (*Essai*, éd 2ᵉ, n. 155) indica residuo de $a \uparrow [p-1)/2]$ (mod$p$) cum symbolo $\left(\frac{a}{p}\right)$, que hodie es communi ad omni auctore, sed apud LEGENDRE tali symbolo habe aut valore 1 aut valore —1, nam definitione ·03 es posteriore. Nos ute simbolo $\mathrm{J}(a,p)$, que es magis consentaneo ad notatione de Form.}

·1 $\mathrm{J}(1,p) = 1$

·2 $\mathrm{J}(-1,p) = (-1) \uparrow [(p-1)/2]$

·21 $\mathrm{J}(-1,p) = 1 \,.=.\, p \varepsilon 4\mathrm{N}_0+1 \;:\; \mathrm{J}(-1,p) = -1 \,.=.\, p \varepsilon 4\mathrm{N}_0+3$

{Ce theorema es noto ad FERMAT, sed primo demonstratione pertine ad EULERO (*Opusc. Anal.* t. 1. p. 64, *Comm. Petrop.* n. 5, a. 1759, p. 5, et n. 18, a. 1774, p. 112 = Comm. Ar. coll. 1, p. 210, 477) Vide et GAUSS, Disqu. Arith., art. 108-111,}

·3 $\mathrm{J}(ab,p) = \mathrm{J}(a,p) \times \mathrm{J}(b,p)$

·4 $a \varepsilon b+\mathrm{n}p \,.\supset.\, \mathrm{J}(a,p) = \mathrm{J}(b,p)$

·5 $\mathrm{J}(2,p) = (-1) \uparrow [(p^2-1)/8]$

·51 $\mathrm{J}(2,p) = 1 \,.=.\, p \varepsilon (8\mathrm{N}_0+1) \cup (8\mathrm{N}_0+7):$
$\mathrm{J}(2,p) = -1 \,.=.\, p \varepsilon (8\mathrm{N}_0+3) \cup (8\mathrm{N}_0+5)$

{·5·51 FERMAT novi ce theorema sed non trade demonstratione. (*Op. math.*, p. 168). EULERO fac conatu ut demonstra illo sed frusta. Primo demonstratione rigoroso pertine ad LAGRANGE (*Nouv. Mém. de l'Ac. de Berlin*, a. 1775. pag. 349, 351 = Oeuvres t. 3, p, 771. Vide et GAUSS, Disq. Arith. art. 112, 116, LEGENDRE, Essai, 2ᵉ éd. n. 148, 386; STIELTJES, Neuw Arch. t. 9, a. 1882, p. 193, Ann. d. Toulouse, t. 11 A, a. 1887, p. 5.

·6 $\mathrm{J}(3,p) = 1 \,.=.\, p \varepsilon (12\mathrm{N}_0+1 \cup 12\mathrm{N}_0+11):$
$\mathrm{J}(3,p) = -1 \,.=.\, p \varepsilon (12\mathrm{N}_0+5 \cup 12\mathrm{N}_0+7)$

·7 $\mathrm{J}(5,p) = 1. =. p \varepsilon (20\mathrm{N}_0+1 \cup 20\mathrm{N}_0+9 \cup 20\mathrm{N}_0+11 \cup 20\mathrm{N}_0+19):$
$\mathrm{J}(5,p) = -1. =. p \varepsilon (20\mathrm{N}_0+3 \cup 20\mathrm{N}_0+7 \cup 20\mathrm{N}_0+13 \cup 20\mathrm{N}_0+17)$

·8 $\mathrm{J}(7,p) = 1 \;.=.\; p \,\varepsilon\, (28\mathrm{N}_0+1 \cup 28\mathrm{N}_0+3 \cup 28\mathrm{N}_0+9 \cup 28\mathrm{N}_0+19 \cup 28\mathrm{N}_0+25 \cup 28\mathrm{N}_0+27)$:
$\mathrm{J}(7,p) = -1 \;.=.\; (28\mathrm{N}_0+5 \cup 28\mathrm{N}_0+11 \cup 28\mathrm{N}_0+13 \cup 28\mathrm{N}_0+15 \cup 28\mathrm{N}_0+17 \cup 38\mathrm{N}_0+23)$

{·6·7·8 Ce propositiones que es casu particulari de « lege de reciprocitate de residuos quadratico » (10·4) es noto multo ante que demonstratione de ce theorema. P·6 circa residuo 3 es noto ad FERMAT (*Opera math.* t. 2, p. 857) sed EULERO primo demonstra illo et « eo magis es mirandum demostrationem propositionum ad residua +2 et —2 pertinentium, prorsus similibus artificiis innexas, semper ipsius sagacitatem fugisse » (GAUSS, *Disqu. Arith.* art. 120). LAGRANGE postea demonstra ce P et P·7·8 circa residuo 5 et 7, sed illo non investiga ultra (Mémoires de l'Ac. de Berlin 1775, p. 352);. Vide et BRICARD, *Sur le caractère quadratique du nombre* 3 etc., Nouv. Ann. s. 3ᵉ, t. 16, a. 1887, p. 546}.

✻ 10. $p,q \,\varepsilon\, \mathrm{Np} - \iota 2 \;.\; a,b \,\varepsilon\, \mathrm{n} \;.\supset:$

·1 $a \,\varepsilon\, b+\mathrm{n}p \;.\supset.\; \mathrm{J}(a,p) = (-1)\uparrow\Sigma[\mathrm{E}(2ra/p)|r, 1\cdots(p-1)/2]$

{LEGENDRE, *Essai*, 2ᵉ éd. nn 381, 382}

·2 $a \,\varepsilon\, 2\mathrm{N}_0+1 - \mathrm{N}_1\times p \;.\supset.\; \mathrm{J}(a,p) = (-1)\uparrow\Sigma[\mathrm{E}(ra/p)|r, 1\cdots(p-1)/2]$

{LEGENDRE, *Essai*, 2ᵉ éd. nn. 383, 384}

·3 $\mathrm{J}(q,p) = (-1)\uparrow\mathrm{Num}\{1\cdots(p-1)/2 \cap x\ni[\mathrm{rest}(xq,p) > p/2]\}$

« Lemma de Gauss » (Werke t 2, p, 3) - Ce P es extenso a P. GAZZANIGA in R. Istituto Veneto s. 6, 4², 1886, p. 1271.

·31 $\mathrm{J}(q,p) = \mathrm{sgn}\Pi\{[xq/p - \mathrm{E}(xq/p+/2)]|x, 1\cdots(p-1)/2\}$

·32 $\mathrm{J}(q,p) = \mathrm{sgn}\Pi\{[\sin(2xq\pi/p)]/\sin(2x\pi/p)|x, 1\cdots(p-1)/2\}$

{EISENSTEIN, *J, f. Math*, t. 29, a. 1845, p. 177.}

·33 $\mathrm{J}(q,p) = \Pi\{\Pi[(h/p-k/q)(h/p+k/q-/2)|h, 1\cdots(p-1)/2]|k, 1\cdots(q-1)/2\}$

·34 $\mathrm{J}(q,p) = \Pi\{\Pi[(h/p-k/q)|h, 1\cdots(p-1)/2]|k, 1\cdots(q-1)/2\}$

{KRONECHER, *Berlin. Ber.* t. 7, a. 1884, p. 519}

·4 $\mathrm{J}(p,q) = (-1)\uparrow[(p-1)(q-1)/4] \times \mathrm{J}(q,p)$

{Ce propositione es « lege de reciprocitate de residuos quadratico » EULERO inveni illo sed non demonstra :

« Existente *s* numero quocumque primo, dividantur tantum quadrata imparia

1, 9, 25, 49,...

per divisorem $4s$, notenturque residua, quae omnia erunt formae $4q+1$, quorum quodvis littera *a* indicetur, reliquorum autem numerorum, formae $4q+1$, qui inter residua non occurrunt, quilibet littera ***A*** indicetur, quo facto si fuerit divisor numerus primus

formae	tum est
$4ns+a$	$+s$ residuum et $-s$ residuum
$4ns-a$	$+s$ residuum et $-s$ non-residuum
$4ns+A$	$+s$ non-residuum et $-s$ non-residuum
$4ns-A$	$+s$ non-residuum et $-s$ residuum ».

(Opusc. Anal., t. 1, a. 1772).

Primo demonstratione pertine ad LEGENDRE, sed non es rigoroso. GAUSS trade septem demonstratione de ce « theorema fundamentali » :

1°. demonstratione (Disqu. Arith. art. 131-151) es ducto cum methodo de inductione ex theorema

$p \varepsilon\, 8N_0+1 \;.\supset.\; \exists\, Np \cap 1 \cdots (p-1) \cap x \ni [J(p,x) = -1].$

2°. demonstratione (Disqu. Arith. art. 262) es deducto ex theoria de formas quadratico;

4°. et 6.° (Werke, t. 2, p, 9 et 55) ex teoria de divisione de circulo;

7°. (Werke, t. 2, p. 234) ex theoria de congruentias de gradu superiore;

3°. et 5.° ex P 10·3 (lemma de GAUSS).

EISENSTEIN (J. f. Math, t. 28, a. 1844, p. 246) da demonstratione geometrico.

GENOCCHI (Mém. de l'Ac. de Belgique, t. 25, a. 1853 (1852), cap. 13; vide et Comptes Rendus de l'Ac. de Paris t. 90, a. 1880, p. 350; et J. f. Math, 1892) funda simplice demonstratione de lege de reciprocitate supra relatione

$$2E(hq/p) = \Sigma\{[1+\mathrm{sgn}(h/p-k/q)] \mid k, 1\cdots(q-1)/2\},$$
$$2E(hq/p+/2) = \Sigma\{[1+\mathrm{sgn}(h/p+k/q-/2)] \mid k, 1\cdots(q-1)/2\}$$

(Circa relationes analogo v. HACKS, Acta Math, t. 12, 1888, p. 109; BUSCHE, *Ueber eine Beveismethode in der Zahlentheorie*, Göttingen, 1883; STEIN, J. f. Math, t. 106, a. 1890, p. 337).

Circa alio simplice demonstratione v. BUNIAKOWSKY, Bull. St-Pét., t. 14, a. 1869, p. 432; — ZELLER, Monatsberichte der Ber. Ak., a. 1872; — ZOLOTAREFF, Nouvelles Annales, s. 2, t. 11, a. 1872, p. 354; — SCHERING, Gött. Nachr. a. 1879, p. 217.

KRONECKER publica vario articulo circa lege de reprocitate (V. Kronecker's Werke). Simplicissimo es demonstratione de ce auctore, posito supra P. 10·33·34 (Berl. Berichte, t. 7, a. 1884, p. 519).

Ad publicationes citato nos adde

KRONECKER, Berl. Monatsber, a. 1880, p. 686, p. 854; — SYLVESTER, Comptes Rendus de l'Ac. de Paris, t. 90, a. 1880, p. 1053, 1104; t. 91, p. 154; — THOMAE, Zeitsch. f. Math. v. Ph, t. 26, a. 1881, p. 134; — STIELTJES, Nieuw Arch. t. 9, a. 1882, p. 193; — SCHERING, Acta Math, t. 1, a. 1883, p. 153; — KRONECKER, Berl. Ber., a. 1884, p. 519; J. f. Math., t. 96. a. 1884, p. 348; Berl. Ber., a. 1884, p. 645; J. f. Math., t. 97, a. 1884. p. 93; Berl. Ber. a. 1885, p. 383; — GEGENBAUER, Wien Ber. t. 91, a. 1885, p. 11; t. 92, a. 1885, p. 876; — SCHERING, Berl. Ber., a. 1885, p. 113; — KRONECKER, Berl. Ber., a. 1885, p. 117; — KUMMER, J. f. Math., t. 100, a. 1886, p. 10; — HERMES, Hoppe Arch., t. 5, a. 1887, p. 190; — LERCH, Teixeira J., t. 8, a. 1887, p. 137; — GEGENBAUER, Wien Ber. t. 97, a. 1888, p. 427; — BUSCHE, J. f. Math., t. 103, a. 1888, p. 118; — KRONECKER, J. f. Math., t. 104, a. 1889, p. 348; — TAFELMACHER, Diss. Göttingen, a. 1889; — LIPSCHITZ, C. R. de l'Ac. de Paris, t. 108, a. 1889, p. 489; — MANDL, Monatsber. f. Math., t. 1, a. 1890, p. 465; — PÉPIN, Acc. Pont. dei N. Lincei, t. 43, a. 1890, p. 192; — FRANKLIN, Messenger of. Math,, t. 19, a. 1890, p. 176; — FIELDS, American J. t. 13, a. 1890, p. 189; — BUSCHE J. f, Math., t. 106, a. 1890, p. 65; — KRONECKER, J. f. Math., t. 106. a. 1890, p. 346; — MATROT, Assoc. Franç., Limoges XIX, a. 1890, p. 79; — LUCAS, Assoc. Franç., Limoges XIX_1, a. 1890, p. 147; Mélanges math. et. astr., S. Pétersb. t. 7, 1891, p. 65; — GEGENBAUER, Wien Ber, t. 100, a. 1891, p. 855; p. 1072; — SCHMIDT, J. f. Math., t. 111, a. 1893, p. 107; GEGENBAUER, Wien Ber., t. 103, a. 1894, p. 285; — BANG. Nyt Tidss. for Math., t. 5 B., a. 1894, p. 92; — BUSCHE,

Hamb. Mitt.. t. 3, a. 1896, p. 233; — LANGE, Leipz. Ber., t. 48, a. 1896, p. 629; — LERCH, Bull. Int. Prague, 1896; — LANGE, Leipz. Ber., t. 49, a. 1897, p. 607; — STERNEK, Recueil math. de Moscou. (in russo), t. 20, a. 1898, p. 267; — PÉPIN, Acc. P. d. N. Lincei, t. 51, a. 1898, p. 123; — ALEXEJEVSKY, Charkow Ges. t. 6, 1898, p. 200 (in russo); PÉPIN, Mem. Acc. d. N. Lincei, t. 16, a. 1900, p. 229; — FISCHER, Monatsb., f. Math. t. 11, a. 1900, p. 176; — GAUSS, *Sechs Beweise des Fundamentaltheorems über quadratische reste*, hrsg. von NETTO, (Ostwalds kl. N° 122), Leipzig: W. Engelmann, a. 1901.

* 11. $a,b \varepsilon$ n . $m,n \varepsilon\ 2N_0+1$.⊃:

·0 $J(a,m) = \Pi[J(a,p)|p, Np \cap m/N_1]$ Df

$J(a,m)$ es appellato *symbolo de Jacobi.*

·01 $J(a,-m) = J(a,m)$ Df

·1 $J(a \times b,m) = J(a,m) \times J(b,m)$

·2 $a \varepsilon\ b+np$.⊃. $J(a,m) = J(b,m)$

·3 $J(1,m) = 1$

·4 $J(-1,m) = (-1)\upharpoonright[(m-1)/2]$

·5 $J(2,m) = (-1)\upharpoonright[(m^2-1)/8]$

·6 $a \varepsilon N_1$.⊃. $J(a\ m) = \text{sgn}\Pi\{[\text{rest}(ra,m)-m]|r, 1\cdots(m-1)/2 \cap x\ni[\text{rest}(xa,m)>m/2]\}$ Dfp

{Ita SCHERING et KRONECKER defini symbolo de JACOBI (Berl. Ber. a. 1876, p. 330)

·7 $m \varepsilon$ n . $J(a,m) = \Pi\{[\sin(2ax\pi/m)/\sin(2x\pi/m)]|x, 1\cdots(\text{mod}\,m-1)/2\}$ Dfp

·8 $m,n \varepsilon\ 2N_0+1$.⊃. $J(m,n) = \Pi\{\Pi[4\sin(h\pi/m+k\pi/n)\times \sin(h\pi/m-k\pi/2)|h,1\cdots(m-1)/2]|k, 1\cdots(n-1)/2\}$

·9 $m,n \varepsilon\ 2N_0+1$.⊃. $J(m,n) = (-1)\upharpoonright[(m-1)(n-1)/4] \times J(n,m)$.

{·9. Extensione de (P10·4) lege de reciprocitate. Ut pote determina valore de $J(m,n)$ es regulas posito aut supra algorithmo de Euclide aut supra algorithmo de fractione continuo, v. GAUSS, Werke, t. 2, p. 61 et sequ.; EISENSTEIN, J. f. Math.,

t. 27, a. 1844, p. 317; LEBESGUE, J. de Math., t. 12, a. 1847, p. 497; ZELLER, Gött. Nach., a. 1879, p. 197; SCHERING, Gött. Nach., a. 1879, p. 217; GEGENBAUER, Wien Berich., a. 1880, p. 931, et a. 1881, p. 1089., KRONECKER, Berl. Ber., a. 1884, p. 530; HEINITZ, Diss. Gött., a. 1893}.

* 12. $p \varepsilon \mathrm{Np} - \iota 2 \,.\, r,n \varepsilon \mathrm{n} \,.\, \mathrm{J}(r,p) = 1 \,.\, \mathrm{J}(n,p) = -1 \,.\supset:$

$\mathrm{Num}\{1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = 1 \,.\, \mathrm{J}(r+x,p) = 1]\} = \mathrm{E}[(p-2)/4]$

$\mathrm{Num}\{1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = 1 \,.\, \mathrm{J}(r+x,p) = -1]\} = \mathrm{E}[(p+2)/4]$

$\mathrm{Num}\{1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = -1 \,.\, \mathrm{J}(r+x,p) = 1]\} = \mathrm{E}[(p-1)/4]$

$\mathrm{Num}\{1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = -1 \,.\, \mathrm{J}(r+x,p) = -1]\} = \mathrm{E}[(p-1)/4]$

$\mathrm{Num}\{1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = 1 \,.\, \mathrm{J}(n+x,p) = 1]\} = \mathrm{E}[(p-1)/4]$

$\mathrm{Num}\{1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = 1 \,.\, \mathrm{J}(n+x,p) = -1]\} = \mathrm{E}[(p-1)/4]$

$\mathrm{Num}\{1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = -1 \,.\, \mathrm{J}(n+x,p) = 1]\} = \mathrm{E}[(p+2)/4]$

$\mathrm{Num}\{1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = -1 \,.\, \mathrm{J}(n+x,p) = -1]\} = \mathrm{E}[(p-2)/4]$

v. meo scripto *Un metodo per la risoluzione*, etc. Napoli R. 1903, p. 154.

$p \varepsilon \mathrm{Np} - \iota 2 \,.\supset.\, \exists 1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = 1 \,.\, \mathrm{J}(x+1,p) = -1$

$p \varepsilon \mathrm{Np} \frown \mathrm{N}_1 + 3 \,.\supset.\, \exists\, 1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = -1 \,.\, \mathrm{J}(x+1,p) = 1]$

———————— $.\supset.\, \exists\, 1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = \mathrm{J}(x+1,p) = -1]$

$p \varepsilon \mathrm{Np} \frown \mathrm{N}_1 + 5 \,.\supset.\, \exists\, 1\cdots(p-1) \frown x \ni [\mathrm{J}(x,p) = \mathrm{J}(x+1,p) = 1]$

* 13·1 $p \varepsilon \mathrm{Np} \frown 8\mathrm{N}_0 + 3 \,.\supset.$

$\mathrm{Num}\{1\cdots(p-3)/4 \frown x \ni [\mathrm{J}(x,p) = 1]\} = (p-3)/8$

·2 $p \varepsilon \mathrm{Np} \frown 8\mathrm{N}_0 + 7 \,.\supset.$

$\mathrm{Num}\{(p-3)/4\cdots(p-3)/2 \frown x \ni [\mathrm{J}(x,p) = 1]\} = (p+1)/8$

{·1·2 BRICARD, Intermédiaire des M., t. 3, a. 1896, p. 62; t. 6, a. 1902, p. 417}

* 14·1 $m \varepsilon 2\mathrm{N}_1 + 1 - \mathrm{N}_1 \times \mathrm{N}_1^2 \,.\, a \varepsilon \mathrm{n}^2 + \mathrm{n}m - \mathrm{n}m \,.$

$u \varepsilon \iota 1 \cup \iota(-1) \mathrm{F} \mathrm{Np} \,.\supset.$

$\mathrm{Num}\{1\cdots(m-1) \frown \mathrm{n}^2 - a + \mathrm{n}m \frown x \ni [p \varepsilon \mathrm{Np} \frown m/\mathrm{N}_1 \,.\supset_p .$

$\mathrm{J}(x,p) = u_p \,]\} = \Pi\{\mathrm{E}[(p-u_p)/4] \,|\, p, \mathrm{Np} \frown m/\mathrm{N}_1\}$

{v. meo scripto *Applicazione della teoria* etc., Napoli R., a. 1904, p. 135}

* 15· $p \varepsilon \mathrm{Np} - \iota 2 \,.\, a \varepsilon \mathrm{n} \,.\, \mathrm{J}(a,p) = 1 \,.\supset:$

·1 $p \varepsilon 4\mathrm{N}_0 + 3 \,.\supset.\, a \uparrow [(p+1)/4] \,\varepsilon\, \mathrm{n} \frown x \ni (x^2 \varepsilon\, a + \mathrm{n}p)$

·2 $p \varepsilon 8\mathrm{N}_0+5 \,.\, a\upharpoonright[(p-1)/4] \varepsilon 1+\mathrm{n}p \,.\supset.$
$a\upharpoonright[(p+3)/8] \varepsilon \mathrm{n}\frown x \ni (x^2 \varepsilon a+\mathrm{n}p$

·3 ——— $.\, a\upharpoonright[(p-1)/4] \varepsilon -1+\mathrm{n}p \,.\supset.$
$2\upharpoonright[(p-1)/4]\, a\upharpoonright[(p+3)/8] \varepsilon \mathrm{n}\frown x\ni(x^2 \varepsilon a+\mathrm{n}p)$

}·1·2·3 LEGENDRE, *Essai*, 2[e] éd., n. 185{

·4 $p \varepsilon 8\mathrm{N}_0+5 \,.\supset.\, a\upharpoonright[(p+3)/8] \times \{ a\upharpoonright[(p-1)/4]+3 \} \upharpoonright[(p-1)/4]$
$\varepsilon\, \mathrm{n}\frown x\ni(x^2 \varepsilon a+\mathrm{n}p)$

}TONELLI, Lincei R., a. 1892, 1[0] sem., p. 116{

✻ 16. $p \varepsilon \mathrm{Np}-\iota 2 \,.\, a,b \varepsilon \mathrm{n} \,.\, \mathrm{J}(a,p) = 1 \,.\, \mathrm{J}(b,p) = -1 \,.$
$m \varepsilon 2\mathrm{N}_0+1 \,.\, r,s \varepsilon \mathrm{N}_1 \,.\, p = 2^s m+1 \,.\supset:$

·1 $u \varepsilon \mathrm{N}_1 \frown x\ni(a^m b^{2m.x} \varepsilon 1+\mathrm{n}p) \,.\supset.$
$b^{mu}\, a\upharpoonright[(m+1)/2] \varepsilon \mathrm{n}\frown x\ni(x^2 \varepsilon a+\mathrm{n}p)$

·2 $k \varepsilon \mathrm{n}\frown x\ni[\mathrm{J}(x+1,p) = 1 \,.\, \mathrm{J}(x-1,p) = -1] \,.\, v \varepsilon \mathrm{nFN}_0 \,.$
$v_0 \varepsilon k+a\upharpoonright(2^{s-2}m)+\mathrm{n}p \,.\, v_r \varepsilon k+a\upharpoonright(2^{s-r-2}m) \times$
$\Pi[v_h \upharpoonright(2^{s-r-h-1}m) | h, 1\cdots(r-1)]+\mathrm{n}p$
$.\supset.\, a\upharpoonright[(m+1)/2]\, \Pi[v_r \upharpoonright(2^r m) \,|\, r, 0\cdots(s-1)] \varepsilon \mathrm{n}\frown x\ni(x^2 \varepsilon a+\mathrm{n}p)$

}·1·2 TONELLI, Lincei R., a. 1892, 1[0] sem., p. 116{

·3 $p \varepsilon 4\mathrm{N}_0+1 \,.\, k \varepsilon \mathrm{n}\frown x\ni(x^2 \varepsilon a+\mathrm{n}p) \,.\supset.$
$kb\upharpoonright(2^{s-2}m) \varepsilon \mathrm{n}\frown x\ni(x^2 \varepsilon -a+\mathrm{n}p)$

}TONELLI, Lincei R., a. 1892, 1[0] sem., p. 116{

✻ 17. $p \varepsilon \mathrm{Np}-\iota 2 \,.\, k,a \varepsilon \mathrm{n} \,.\, \mathrm{J}(a,p) = 1 \,.\, \mathrm{J}(k^2-a,p) = -1 \,.\supset:$

·1 $\{[k+\surd(k^2-a)]\upharpoonright[(p+1)/2] + [k-\surd(k^2-a)]\upharpoonright[(p+1)/2\Pi]\}$
$\varepsilon\, \mathrm{n}\frown x\ni(x^2 \varepsilon a+\mathrm{n}p)$

·2 $\surd a\{(k+\surd a)\upharpoonright[(p-1)/2] - (k-\surd a)\upharpoonright[(p-1)/2]\}/2$
$\varepsilon\, \mathrm{n}\frown x\ni(x^2 \varepsilon a+\mathrm{n}p)$

}·1·2 v. meo scripto *Un metodo*, etc., Napoli R., a. 1903, p. 154{

·3 $2\Sigma\{a^r \Sigma[1\cdots(p-1)/2]^{2r-1} | r, 1\cdots(p-1)/2\} \varepsilon \mathrm{n}\frown x\ni(x^2 \varepsilon a+\mathrm{n}p)$

}v. meo scripto *Formole*, etc., Napoli R. a. 1905, p. 13{

Propositiones de nn. 15, 16, 17 enuntia vario methodo ut resolve congruentia de secundo gradu cum modulo primo. GAUSS trade duo methodo ut inveni solutiones, altero (Disqu. Arith., art. 319-322), dicto methodo de *excludente*, exige cognitione de non residuo de plure numero, altero (Disqu. Arith. art. 327) nite in theoria de formas quadratico. Methodos ut

inveni numeros positivo, que non supera modulo et satisfac ad congruentia *(radices)*, exige plure conatu et methodo de excludente es in tali casu magis idoneo que omni alio. Ut inveni uno quolibet solutione suffice ute formulas de TONELLI (16·2), aut meo (17·1 vel 17·2), pro que conatus es pauco. Meo formula 17·3 monstra postea solutione de congruentia sine ullo conatu, sed illo es pauco utili in practica.

✻ 18 $n \varepsilon \mathrm{N}_1 \,.\, p \varepsilon \mathrm{Np} - \iota 2 \,.\, a \varepsilon \mathrm{n} \,.\, \mathrm{J}(a,p) = 1 \,.\, l \varepsilon \mathrm{n} \cap x \ni (x^2 \varepsilon\, a + \mathrm{n}p) \,.\supset:$

·1 $r \varepsilon\, [(l+\sqrt{a})^n - (l-\sqrt{a})^n]/(2\sqrt{a}) + \mathrm{n}p \,.$
$s \varepsilon [(l+\sqrt{a})^n + (l-\sqrt{a})^n]/2 + \mathrm{n}p \,.\supset.$
$\mathrm{n} \cap x \ni (x^2 \varepsilon\, a + \mathrm{n}p^n) = \mathrm{n} \cap \{x \ni (rx \varepsilon\, s + \mathrm{n}p^n) \cup x \ni (rx\, \varepsilon -s + \mathrm{n}p^n)]$
{LEGENDRE, *Essai*, 2[e] éd. n. 187{

·2 $(l \uparrow p^{n-1}) a \uparrow [(p^n - 2p^{n-1} + 1)/2]\ \varepsilon\ \mathrm{n} \cap x \ni (x^2 \varepsilon a + \mathrm{n}p^n)$
{TONELLI, Lincei R., a. 1893, 1[0] sem., p. 259{

✻ 19. $n \varepsilon \mathrm{N}_1 \,.\, p \varepsilon\, \mathrm{Np} - \iota 2 \,.\, a \varepsilon \mathrm{n} \,.\, \mathrm{J}(a,p) = 1 \,.\supset:$

·1 $p \varepsilon\, 4\mathrm{N}_0 + 3 \,.\supset.\, a \uparrow [(p^n - p^{n-1} + 2)/4]\ \varepsilon\ \mathrm{n} \cap x \ni (x^2 \varepsilon\, a + \mathrm{n}p^n)$

·2 $p \varepsilon\, 8\mathrm{N}_0 + 5 \,.\supset.$
$\{a \uparrow [(p^n - p^{n-1} + 4)/8]\}\{a \uparrow [(p-1)/4] + 3\{\uparrow [(p^n - p^{n-1})/4]\ \varepsilon$
$\mathrm{n} \cap x \ni\ (x^2 \varepsilon a + \mathrm{n}p^n)$
{·1·2 TONELLI, Lincei R., a. 1893, 1[0] sem., p. 259{

✻ 20. $\mathrm{Hp}19 \,.\, m \varepsilon\, 2\mathrm{N}_0 + 1 \,.\, r,s \varepsilon \mathrm{N}_1 \,.\, p = 2^s m + 1 \,.\supset:$

·1 $b \varepsilon \mathrm{n} \,.\, \mathrm{J}(b,p) = -1 \,.\, u \varepsilon\, \mathrm{N}_1 \cap x \ni \{[a \uparrow (p^{m-1} m)] b \uparrow (2p^{n-1} m x)\ \varepsilon$
$1 + \mathrm{n}p^n\{ \,.\supset.\, [b \uparrow (p^{n-1} m u] a \uparrow [(p^{n-1} m + 1)/2]\ \varepsilon\ \mathrm{n} \cap x \ni (x^2 \varepsilon\, a +$
$\mathrm{n}p^n)$
{TONELLI, Lincei R., a. 1892, 1[0] sem. p. 116{

·2 $k \varepsilon\, \mathrm{n} \cap x \ni [\mathrm{J}(x+1,p) = 1 \,.\, \mathrm{J}(x-1,p) = -1] \,.\, v \varepsilon \mathrm{nFN}_0 \,.$
$v_0 \varepsilon\, k + a \uparrow (2^{s-2} m) + \mathrm{n}p \,.\, v_r\ \varepsilon\ k + \mathrm{n}p + [a \uparrow (2^{s-r-2} m)] \times$
$\Pi[v_h \uparrow (2^{s-r-h-1} m) | h, 1 \cdots (r-1)] \,.\supset.\, \{a \uparrow [(p^{n-1} m + 1)/2]\} \times$
$\Pi[v_r \uparrow (2^r p^{n-1} m) | r, 0 \cdots (s-1)]\ \varepsilon\ \mathrm{n} \cap x \ni (x^2 \varepsilon\, a + \mathrm{n}p^n)$
{TONELLI, Lincei R., a. 1893, 1[0] sem. p. 259{

·3 $k \varepsilon \mathrm{n} \,.\, \mathrm{J}(k^2 - a,p) = -1 \,.\supset.$
$\{a \uparrow [(p^n - 2p^{n-1} + 1)/2]\}\{[k + \sqrt{(k^2 - a)}] \uparrow [p^{n-1}(p+1)/2] +$
$[k - \sqrt{(k^2 - a)}] \uparrow [p^{n-1}(p+1)/2]\{\ \varepsilon\ \mathrm{n} \cap x \ni (x^2 \varepsilon\, a + \mathrm{n}p^n)$

·4 $\text{Hp}\cdot 3 .\supset. \sqrt{a}\{(k+\sqrt{a})\uparrow[p^{n-1}(p-1)/2]-(k-\sqrt{a})[p^{n-1}(p-1)/2]\}/2$
$\varepsilon\ \text{n}\cap x\ni(x^2\varepsilon a+\text{n}p^n)$

{·3·4 v. meo scripto *Applicazione*, etc, Napoli R., a. 1904, p. 135}

* 21. $n\varepsilon\ \text{N}_1+1 \,.\, p\varepsilon\ \text{Np}-\iota 2 \,.\, k\varepsilon\ \text{n}\cap x\ni(x^2\varepsilon\ a+\text{n}p^{n-1}) .\supset:$

·1 $b\varepsilon\ \text{n}\cap x\ni[(k^2-a)/p^{n-1}+2kx\varepsilon\text{n}p\} .\supset.$
$a+bp^{n-1}\ \varepsilon\ \text{n}\cap x\ni(x^2\varepsilon\ a+\text{n}p^n)$

* 22·1 $a\varepsilon\ 2\text{n}+1 .\supset: \text{n}\cap x\ni(x^2\varepsilon\ a+2\text{n}) = 2\text{n}+1$

·2 $a\varepsilon\ 4\text{n}+1 \cup 4\text{n}-1 .\supset. \text{n}\cap x\ni(x^2\varepsilon\ a+4\text{n}) = 4\text{n}+1 \cup 4\text{n}+3$

·3 $a\varepsilon\ 8\text{n}+1 .\supset. \text{n}\cap x\ni(x^2\varepsilon a+8\text{n}) = 8\text{n}+1\cup 8\text{n}+3\cup 8\text{n}+5\cup 8\text{n}+7$

·4 $r\varepsilon\text{N}_0 .\supset: \exists\ \text{n}\cap x\varepsilon(x^2\varepsilon\ a+2^{r+3}\text{n}) .=. a\varepsilon\ 8\text{n}+1$

·5 $r\varepsilon\text{N}_0 \,.\, a\varepsilon\ 8\text{n}+1 .\supset. \text{Num}[1\cdots(2^{r+3}-1)\cap x\ni(x^2\varepsilon a+2^{r+3}\text{n})] = 4$

·6 $\text{Hp}\cdot 5 \,.\, u\varepsilon\ \text{n}\cap x\ni(x^2\varepsilon\ a+2^{r+3}\text{n}) .\supset. \text{n}\cap x\ni(x^2\varepsilon a+2^{r+3}\text{n}) =$
$(u+2^{r+2}\text{n})\cup(-u+2^{r+2}\text{n})$

{·6 v. GAUSS Disqu. Arith. art. 103; LEGENDRE, *Essai*, 2[e] éd. n. 189}

·7 $a\ \varepsilon\ 8\text{n}+1 \,.\, m\ \varepsilon\ \text{N}_1 \,.\, s=\text{mp}(2,a-1) .\supset.$
$1+(a-1)/2\Sigma\{\text{C}(2r,r)[(1-a)/4]^r/(r+1)|r,0\cdots\text{E}[(m-2)/(s-2)-1\}$
$\varepsilon\ \text{n}\cap x\ni(x^2\ \varepsilon\ a+2^m\text{n})$

{·7 Ce formula pertine ad LEGENDRE (*Essai*, 2[e] éd. nn. 350-2); circa demonstratione rigoroso de illo v. meo scripto: *Estensione di un metodo di Legendre*, etc., Napoli R., 1905.}

* 23 $m\varepsilon\text{N}_1 \,.\, a\varepsilon\text{n} \,.\, \text{D}(a,m) = 1 .\supset:$

·1 $m\varepsilon\ 2\text{N}_0+1 \cup 2(2\text{N}_0+1) .\supset: \exists\ \text{n}\cap x\ni(x^2\varepsilon\ a+\text{n}m) .=.$
$p\varepsilon\text{Np}-\iota 2 \cap m/\text{N}_1 .\supset_p. \text{J}(a,p)=1$

·11 $\text{Hp}\cdot 1 .\supset. \text{Num}[1\cdots(m-1)\cap x\ni(x^2\varepsilon\ a+\text{n}m)] =$
$2\uparrow\text{Num}(\text{Np}-\iota 2 \cap m/\text{N}_1)$

·2 $m\varepsilon\ 4(2\text{N}_0+1) .\supset: \exists\text{n}\cap x\ni(x^2\varepsilon\ a+\text{n}m) .=: a\varepsilon 2\text{n}+1 :$
$p\varepsilon\text{Np}-\iota 2\cap m/\text{N}_1 .\supset_p. \text{J}(a,p)=1$

·21 $\text{Hp}\cdot 2 .\supset. \text{Num}[1\cdots(m-1)\cap x\varepsilon(x^2\varepsilon\ a+\text{n}m)] =$
$2\uparrow[1+\text{Num}(\text{Np}-\iota 2\cap m/\text{N}_1)]$

·3 $m\varepsilon 8\text{N}_1 .\supset: \exists\text{n}\cap x\ni(x^2\varepsilon\ a+\text{n}m) .=. a\varepsilon\ 8\text{n}+1 :$
$p\varepsilon\text{Np}-\iota 2\cap m/\text{N}_1 .\supset_p. \text{J}(a,p)=1$

·31 $\mathrm{Hp}\cdot 3 \;.\supset.\; \mathrm{Num}[1\cdots(m-1)\frown x\ni(x^2 \varepsilon a+\mathrm{n}m)] =$
$2\uparrow[2+\mathrm{Num}(\mathrm{Np}-\iota 2\frown m/\mathrm{N}_1)]$

✻ 24. $m\varepsilon 2\mathrm{N}_1+1 \;.\; a\varepsilon \mathrm{n}^2+\mathrm{n}m-\mathrm{n}m \;.\; k\varepsilon \mathrm{n} \;.\; n\varepsilon \mathrm{N}_0 \;.\; u,v\varepsilon \mathrm{nFN}_0$
$u_n = \{[k+\surd(k^2-a)]^n - [k-\surd(k^2-a)]^n\}/[2\surd(k^2-a)]$
$v_n = [k+\surd(k^2-a)]^n + [k+\surd(k^2-a)]^n$

·1 $m-\varepsilon\, 3\mathrm{N}_1 \;.\; k\varepsilon\, \mathrm{n}\frown x\ni\{p\varepsilon\, \mathrm{Np}\frown m/\mathrm{N}_1 \;.\supset_p.\; \mathrm{J}(x^2-a,p) =$
$(-1)\uparrow[(p+1)/2]$
$r = \mathrm{mlt}\{[p\uparrow(\max(p,a)-1)][p-(-1)\uparrow[p+1)/2]] \mid p,\, \mathrm{Np}\frown a/\mathrm{N}_1\}$
$.\supset.\; a\uparrow[(\Phi m - r+1)/2]v_r/2 \;\varepsilon\; \mathrm{n}\frown x\ni(x^2\varepsilon\, a+\mathrm{n}m)$

·2 $k\varepsilon\, \mathrm{n}\frown x\ni(p\varepsilon\, \mathrm{Np} \frown a/\mathrm{N}_1 \frown 4\mathrm{N}_0+3 \;.\supset_p.\; x^2-a \;\varepsilon\; \mathrm{n}p) \frown$
$x\ni(p \;\varepsilon\; \mathrm{Np} \frown a/\mathrm{N}_1 \frown 4\mathrm{N}_0+1 \;.\supset_p.\; \mathrm{J}(x^2-a,p) = -1] \;.$
$m_1 = \mathrm{mlt}\{p\uparrow[\max(p,a)-1] \mid p,\, \mathrm{Np}\frown a/\mathrm{N}_1\frown 4\mathrm{N}_0+3\} \;.$
$m_2 = \mathrm{mlt}\{(p+1)/2\; p\uparrow[\max(p,a)-1] \mid p,\, \mathrm{Np}\frown a/\mathrm{N}_1\frown 4\mathrm{N}_0+1\} \;.$
$r = \mathrm{mlt}(m_1,m_2) \;.\supset.\; a\uparrow[(\Phi m - r+1)/2]v_r/2 \;\varepsilon\; \mathrm{n}\frown x\ni(x^2\varepsilon\, a+\mathrm{n}m)$

{·1·2 v. meo scripto *Applicazione*, etc, Napoli R., a. 1904, p. 135}

§ 6 Congruentias binomio

✻ 25. $a,m,n\varepsilon \mathrm{N}_1 \;.\supset.$

·1 $\mathrm{n}\frown x\ni(x^m \varepsilon\, 1+\mathrm{n}a \;.\; x^n \varepsilon\, 1+\mathrm{n}a) = \mathrm{n}\frown x\ni[x\uparrow \mathrm{D}(m,n) \;\varepsilon\; 1+\mathrm{n}a]$

·2 $\mathrm{n}\frown x\ni(x^n \;\varepsilon\; 1+\mathrm{n}a) = \mathrm{n}\frown x\ni[x\uparrow \mathrm{D}(n,\Psi a) \;\varepsilon\; 1+\mathrm{n}a]$

✻ 26. $n\varepsilon \mathrm{N}_1 \;.\; p\varepsilon\, \mathrm{Np}-\iota 2 \;.\supset:$

·1 $\mathrm{n}\frown x\ni(x^n \varepsilon\, 1+\mathrm{n}p) = \mathrm{n}\frown x\ni[x\uparrow \mathrm{D}(n,p-1) \;\varepsilon\; 1+\mathrm{n}p]$

·2 $\mathrm{Num}[(1\cdots(p-1) \frown x\ni(x^n \varepsilon\, 1+\mathrm{n}p)] = \mathrm{D}(n,p-1)$

{GAUSS, Disqu. Arith. art. 60 et sequentes; LEGENDRE, *Essai* etc., 2ᵉ éd., n. 334}

·3 $k\varepsilon\, \mathrm{n}-\mathrm{n}p \;.\supset.\; k\uparrow[(p-1)/\mathrm{D}(n,p-1)] \;\varepsilon\; \mathrm{n}\frown x\ni(x^n \;\varepsilon\; 1+\mathrm{n}p)$

{LEGENDRE, *Essai* etc., 2ᵉ éd. n. 336}

·4 $n\varepsilon\, \mathrm{N}_1\frown(p-1)/\mathrm{N}_1 \;.\; u\varepsilon \mathrm{n} \;.\; n = \min[\mathrm{N}_1\frown x\ni(u^x \;\varepsilon\; 1+\mathrm{n}p)] \;.\supset.$
$\mathrm{n}\frown x\ni(x^n \;\varepsilon\; 1+\mathrm{n}p) = (u^r+\mathrm{n}p) \mid r,\, 1\cdots n$

{GAUSS, Disqu. Arith., art. 65,1°; LEGENDRE, *Essai* etc.,, 2ᵉ éd,, n. 336, 3°.}

❋ 27. $m,n \varepsilon \mathrm{N}_1 \,.\, p \varepsilon \mathrm{Np} - \iota 2 \,.\supset:$

·1 $\mathrm{n} \cap x\ni(x^n \varepsilon 1 + \mathrm{n}p^m) = \mathrm{n} \cap x\ni\{x \upharpoonright \mathrm{D}[n, p^{m-1}(p-1)] \,\varepsilon\, 1 + \mathrm{n}p^m\}$

·2 $n \varepsilon \mathrm{N}_1 \cap p^{m-1}(p-1)/\mathrm{N}_1 \,.\supset.\, \mathrm{n} \cap x\ni(x^n \varepsilon\, 1 + \mathrm{n}p^m) =$
$\{x + yp \upharpoonright [m - \mathrm{mp}(p,n)] + \mathrm{n}p^m\}\{|x, 1 \cdots (p^m - 1) \cap x\ni[x^n \varepsilon\, 1 + \mathrm{n}p^m \,.$
$\exists z\ni(z^n \varepsilon\, 1 + \mathrm{n}p \,.\, x \varepsilon\, z + \mathrm{n}p)], y, 0 \cdots [p \upharpoonright \mathrm{mp}(p,n) - 1]$

·3 $\mathrm{Num}[1 \cdots (p^m - 1) \cap x\ni(x^n \varepsilon\, 1 + \mathrm{n}p^m)] = \mathrm{D}[n, p^{m-1}(p-1)]$

{·2·3 Gauss, Disqu. Arith. n. 85}

·4 $a \varepsilon\, \mathrm{n} \cap x\ni(x^n \,\varepsilon\, 1 + \mathrm{n}p^{m-1}) \,.\, r = \mathrm{mp}(p,n) \,.\supset:$
$r < n - 1 \,.\, h \varepsilon\, \mathrm{n} \cap x\ni[(a^n - 1)/p^{m-1} + xa^{n-1}n/p^r \,\varepsilon\, \mathrm{n}p)] \,.\supset.$
$a + hp^{n-r-1} \,\varepsilon\, \mathrm{n} \cap x\ni(x^n \varepsilon\, 1 + \mathrm{n}p^m)$

·5 $a \varepsilon\, n \cap x\ni(x^n \varepsilon\, 1 + \mathrm{n}p^{m-1}) \,.\, \mathrm{mp}(p,n) = n - 1 \,.\supset.$
$\mathrm{n} \cap x\ni(x^n \varepsilon\, 1 + np^m) = \mathrm{n} \cap x\ni(x^n \varepsilon\, 1 + \mathrm{n}p)$

{·4·5 Gauss, Disqu. Arith., art. 88}

·6 $a \varepsilon\, \mathrm{n} \cap x\ni(x^n \varepsilon\, 1 + \mathrm{n}p) \,.\supset.\, a \upharpoonright p^{m-1} \,\varepsilon\, \mathrm{n} \cap x\ni(x^n \varepsilon\, 1 + \mathrm{n}p^m)$

{Amici, *Sulla risoluzione* etc.. Rend. d. Circolo M. di Palermo, t. 11, a. 1897, p. 44}

Plure propositione de nn. 25, 26, 27 et sequentes pertine ad Eulero, v. Comm. Nov. Petrop. t. 7, p. 49; t. 18. p. 85 et Opusc. Analytica, t. 1.

❋ 28. $n,m \varepsilon \mathrm{N}_1 \,.\supset:$

·1 $\mathrm{n} \cap x\ni(x^n \varepsilon\, 1 + 2^m\mathrm{n}) = \mathrm{n} \cap x\ni(x \upharpoonright \mathrm{D}(n, \Psi 2^m) \,\varepsilon\, 1 + 2^m \mathrm{n}]$

·2 $m \varepsilon \mathrm{N}_1 + 2 \,.\, n \varepsilon\, 1 \cdots (m-2) \,.\supset.$
$\mathrm{Num}[1 \cdots (2^n - 1) \cap x\ni(x \upharpoonright 2^n \varepsilon 1 + \mathrm{n}2^m)] = 2^{n+1}$

·3 $\mathrm{Hp}\cdot 2 \,.\supset.\, 1 \cdots (2^n - 1) \cap x\ni(x \upharpoonright 2^n \,\varepsilon\, 1 + \mathrm{n}2^m) =$
$1 + 2^{m-2} \times [0 \cdots (2^n - 1)] \cup -1 + 2^{m-n} \times (1 \cdots 2^n)$

❋ 29. $p \varepsilon \mathrm{Np} - \iota 2 \,.\, n \varepsilon \mathrm{N}_1 \,.\, a \varepsilon\, \mathrm{n} - \mathrm{n}p \,.\supset:$

·1 $\exists\, \mathrm{n} \cap x\ni(x^n \varepsilon\, a + \mathrm{n}p) \,.=.\, a \upharpoonright [(p-1)/\mathrm{D}(n, p-1)] \,\varepsilon\, 1 + \mathrm{n}p$

·2 $\mathrm{Hp}\cdot 1 \,.\supset.\, \mathrm{Num}[1 \cdots (p-1) \cap x\ni(x^n \varepsilon a + \mathrm{n}p)] = \mathrm{D}(n, p-1)$

{Gauss, Disqu, Arith., art. 60 et sequ,; Legendre, *Essai* etc., 2e éd., n. 334}

·3 $r \varepsilon \mathrm{N}_1 \cap x\ni[nx/\mathrm{D}(n,p-1) \,\varepsilon\, 1 + \mathrm{n}(p-1)/\mathrm{D}(n,p-1)] \,.\supset.$
$\mathrm{n} \cap x\varepsilon(x^n \varepsilon\, a + \mathrm{n}p) = \mathrm{n} \cap x\ni[x \upharpoonright \mathrm{D}(n, p-1) \,\varepsilon\, a^r + \mathrm{n}p]$

GAUSS indica cum $^n\sqrt{a}$ (mod$p$) numeros que satisfac ad congruentia $x^n \varepsilon\ a+\mathrm{n}p$. Ce espressione habe aut nullo aut uno aut plure valore incongruo (mod. p). Hodie nullo auctore ute ce notatione.

·4 $u\varepsilon\mathrm{n}$. $min[\mathrm{N}_1 \frown x \ni (u^x \varepsilon\ 1+\mathrm{n}p)] = n$. $k \varepsilon \mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p)$.⊃.
$\mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p) = (ku^r+\mathrm{n}p) | r`1 \cdots n$

{GAUSS, Disqu. Arith., art. 65,1°.}

·5 $n\varepsilon\ \mathrm{N}_1 \frown (p-1)/\mathrm{N}_1$. $\mathrm{D}[n,(p-1)/n]=1$. $a \upharpoonright [(p-1)/n]\ \varepsilon\ 1+\mathrm{n}p$.
$r\varepsilon\ \mathrm{N}_1 \frown x \ni [nx \varepsilon\ 1+\mathrm{n}(p-1)/n]$.⊃. $a^r \varepsilon\ \mathrm{n} \frown x \ni (x^n \varepsilon a+\mathrm{n}p)$

{GAUSS, Disqu. Arith., art. 67.}

Circa conatus ut inveni solutiones de congruentia $x^n\ \varepsilon\ a+\mathrm{n}p$, ubi $n\varepsilon\ \mathrm{N}_1 \frown (p-1)/\mathrm{N}_1$, v. GAUSS, D. A. art. 67, 68, LEGENDRE. E. 2ᵉ éd. p. 354 (n. 342), p. 355, (n. 346).

·6 ∃ $\mathrm{n} \frown x \ni (x^n+1\ \varepsilon\ \mathrm{n}p)$.=. $(p-1)/\mathrm{D}(n,p-1)\ \varepsilon\ 2\mathrm{N}_0+1$

·7 $'\mathrm{n} \frown x \ni (x^n+1 \varepsilon \mathrm{n}p) = \mathrm{n} \frown x \ni [x \upharpoonright \mathrm{D}(n,p-1)+1\ \varepsilon\ \mathrm{n}p]$

✱ 30. $p\varepsilon\ \mathrm{Np}-\iota 2$. $m\varepsilon \mathrm{N}_1$. $a\varepsilon\ \mathrm{n}-\mathrm{n}p$.⊃.

·1 ∃ $\mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p^m)$.=. $a \upharpoonright [\Phi p^m/\mathrm{D}(n,\Phi p^m)]\ \varepsilon\ 1+\mathrm{n}p^m$

·2 $r\varepsilon\ \mathrm{N}_1 \frown x \ni [nx/\mathrm{D}(n,\Phi p^m)\ \varepsilon\ 1+\Phi p^m/\mathrm{D}(n,\Phi p^m)]$.⊃.
$\mathrm{n} \frown x \ni (x^n \varepsilon a+\mathrm{n}p^m) = \mathrm{n} \frown x \ni [x \upharpoonright \mathrm{D}(n,\Phi p^m)\ \varepsilon\ a^r+\mathrm{n}p^m]$

·3 $n\varepsilon\ \mathrm{N}_1 \frown \Phi p^m/\mathrm{N}_1$.⊃. ∃ $\mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p^m)$.=.
$a \upharpoonright \{[(p-1)p \upharpoonright \mathrm{mp}(p,n)]/n\}\ \varepsilon\ 1+\mathrm{n}p \upharpoonright [\mathrm{mp}(p,n)+1]$

·4 $n\varepsilon\ \mathrm{N}_1 \frown \Phi p^m/\mathrm{N}_1$. ∃ $\mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p^m)$.⊃.
$\mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p^m) = \{x+yp \upharpoonright [m-\mathrm{mp}(p,n)]+\mathrm{n}p^m\} | x,1 \cdots (p^m-1)$
$\frown x \ni [x^n \varepsilon a+\mathrm{n}p^m$. $\exists z \ni (z^n \varepsilon a+\mathrm{n}p$. $x\varepsilon z+\mathrm{n}p)], y,0 \cdots [p \upharpoonright \mathrm{mp}(p,n)-1]$

·5 Hp·4 .⊃. $\mathrm{Num}[1 \cdots (p^m-1) \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p^m)] = \mathrm{D}(n,\Phi p^m)$

·6 Hp·4 . $k\varepsilon\ \mathrm{n} \frown x \varepsilon (x^n \varepsilon\ a+\mathrm{n}p^{m-1})$. $r = \mathrm{mp}(p,n)$.⊃:
$r < m-1$. $h\varepsilon\ \mathrm{n} \frown x \ni [(k^n-a)/p^{m-1} + xk^{n-1}n/p^r\ \varepsilon\ \mathrm{n}p]$.⊃.
$k+hp^{n-r-1}\ \varepsilon\ \mathrm{n} \frown x \ni (x^m \varepsilon a+\mathrm{n}p^m)$

·7 Hp·4 . $k\varepsilon\ \mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p^{m-1})$. $\mathrm{mp}(p,n) = m-1$.⊃.
$\mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p^m) = \mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p)$

·8 $n\varepsilon\ \mathrm{N}_1 \frown (p-1)/\mathrm{N}_1$. $k\varepsilon\ \mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p)$.⊃.
$\{a \upharpoonright [p^m-2p^{m-1}+1)/n]\} \{k \upharpoonright p^{m-1}\ \varepsilon\ \mathrm{n} \frown x \ni (x^n \varepsilon\ a+\mathrm{n}p^m)$

{v. meo scripto, *Applicazione* etc., Napoli R., 1904, n. 7, nota}

* 31. $m, n \varepsilon N_1 \,.\, a \varepsilon 2n+1 \,.\supset:$

·1 $\exists\, n \frown x\ni(x^n \varepsilon\, a+n2^m) \,.=.\, a\upharpoonright[\Psi 2^m / D(n, \Psi 2^m)] \,\varepsilon\, 1+n2^m$

·2 $r \varepsilon N_0 \frown x\ni[nx \varepsilon D(n, \Psi 2^m)+n\Psi 2^m] \,.\supset.$
$n \frown x\ni(x^n \varepsilon\, a+2^m n) = n \frown x\ni[x\upharpoonright D(n, \Psi 2^m) \,\varepsilon\, a^r+2^m n]$

·3 $n \varepsilon 2N_0+1 \,.\, m \varepsilon N_1+1 \,.\, k \varepsilon N_0 \frown x\ni(2^{m-2}x \,\varepsilon\, -1+nn) \,.\supset.$
$a\upharpoonright[(2^{m-2}k+1)/n] \,\varepsilon\, n \frown x\ni(x^n \varepsilon a+2^m n)$

}AMICI, *Sulla risoluzione*, etc., Rend. d. Circolo M. di Palermo, t. 11, a. 1897, p. 46{

·4 $n \varepsilon N_1 \,.\, m \varepsilon N_0+n+2 \,.\supset.\, \exists\, n \frown x\ni(x\upharpoonright 2^n \,\varepsilon\, a+2^m n) \,.=.$
$a \varepsilon 1+2^{n+2} n$

}AMICI, *Risoluzione*, etc., Rend. d. Circolo M. di Palermo, t. 8, a. 1894, p. 198{

·5 $Hp·4 \,.\, a \varepsilon\, 1+2^{n+2} n \,.\, s = mp(2, a-1) \,.\supset.$
$(a+2^n-1)/2^n - \Sigma\{[(1-a)/2^n]^r / r! \Pi[2^n x-1 | x, 1\cdots(r-1)] | r,$
$2\cdots E[(m-2)/(s-n-1)]\} \,\varepsilon\, n \frown x\ni(x\upharpoonright 2^n \,\varepsilon\, a+2^m n)$

}Vide meo scripto: *Estensione* etc., Napoli R., 1905{

6· $Hp·4 \,.\, a \varepsilon\, 1+2^{n+2} n \,.\supset.$
$Num[1\cdots(2^m-1) \frown x\ni(x\upharpoonright 2^n \,\varepsilon\, a+2^m n)] = 2^{n+1}$

}AMICI, *Risoluzione*, etc., Rend. d. Circolo di Palermo, t. 8 a. 1894, p. 198{

·7 $Hp·6 \,.\, v \varepsilon\, n \frown x\ni(x\upharpoonright 2^n \,\varepsilon\, a+2^m n) \,.\supset.$
$n \frown x\ni(x\upharpoonright 2^n \,\varepsilon\, a+2^m n) = (v+2^{m-n} n) \cup -v+2^{m-n} n)$

§7. Theoria de gaussiano. Radices primitivo. Indices

* 32. $a \varepsilon n \,.\, m \varepsilon N_1 \,.\, D(a, m) = 1 \,.\supset.$

·0 $gss(m, n1 = \min[N_1 \frown x\ni(a^x \varepsilon\, 1+nm)]$ Df gss

gss (m, n) = gaussiano de m in basi n. Vocabulo « gaussiano » es introducto a LUCAS, sed ce auctore appella tali numero « gaussiano de n secundum modulo m » (Théor. d. Nombres, 1901, p. 439) GAUSS appella illo « exponente ad que n

pertine ». Circa omni theoria de gaussiano v. meo articulo, *Sui numeri composti*, etc., Ann. di Mat. (s. 3°, t. 9, a. 1903, p. 139).

·1 $\mathrm{N}_0 \frown x \ni (a^x \varepsilon\ 1 + \mathrm{n}m) = \mathrm{N}_0 \times \mathrm{gss}(m,a)$

·2 $r,s \varepsilon \mathrm{N}_0 \,.\supset :\, a^r \varepsilon\ a^s + \mathrm{n}m \,.=.\, r \varepsilon\ s + \mathrm{n} \times \mathrm{gss}(m,a)$

✻ 33. $a \varepsilon 4\mathrm{n}+3-\iota(-1) \,.\, m \varepsilon \mathrm{N}_1 \,.\, n = \mathrm{mp}(2,a+1) \,.\supset:$

·1 $\mathrm{gss}(2,a) = 1$

·2 $m \varepsilon\ 2 \cdots (n+1) \,.\supset.\, \mathrm{gss}(2^m,a) = 2$

·3 $m > n \,.\supset.\, \mathrm{gss}(2^m,a) = 2^{m-n}$

✻ 34. $a \varepsilon\ 4\mathrm{n}+1-\iota 1 \,.\, m \varepsilon \mathrm{N}_1 \,.\, n = \mathrm{mp}(2,a-1)$

·1 $m \leqq n \,.\supset.\, \mathrm{gss}(2^m,a) = 1$

·2 $m \geqq n \,.\supset.\, \mathrm{gss}(2^m,a) = 2^{m-n}$

✻ 35. $p \varepsilon\ \mathrm{Np}-\iota 2 \,.\, a,b \varepsilon\ \mathrm{n}-\mathrm{n}p \,.\supset:$

·1 $\mathrm{gss}(p,a)\ \varepsilon\ \mathrm{N}_1 \frown (p-1)/\mathrm{N}_1$

}FERMAT, a.1640, Oeuvres, t. 2, p. 209{

·2 $\mathrm{Num}[1 \cdots (p-1) \frown x \ni (a^x \varepsilon\ b + \mathrm{n}p)] = (p-1)/\mathrm{gss}(p,a)$

·3 $k,l \varepsilon \mathrm{N}_0 \frown x \ni (a^x \varepsilon\ b + \mathrm{n}p) \,.\supset:\, k \varepsilon\ l + \mathrm{n} \times \mathrm{gss}(p,a)$

Ce P es in Form 1902 (§Np·10·1) sub forma pauco diverso.

✻ 36. $p \varepsilon\ \mathrm{Np}-\iota 2 \,.\, a \varepsilon \mathrm{n}-\mathrm{n}p \,.\, n = \mathrm{mp}[p,\, a \upharpoonright \mathrm{gss}(p,a)-1] \,.\, m \varepsilon \mathrm{N}_1 \,.\supset:$

·1 $m \leqq n \,.\supset.\, \mathrm{gss}(p^m,a) = \mathrm{gss}(p,a)$

·2 $m \geqq n \,.\supset.\, \mathrm{gss}(p^m,a) = p^{m-n}\mathrm{gss}(p,a)$

·3 $\mathrm{gss}(p,{}^m a)\ \varepsilon\ \mathrm{N}_1 \frown p^{m-1}(p-1)/\mathrm{N}_1$

✻ 37. $a \varepsilon \mathrm{n} \,.\, m,n \varepsilon \mathrm{N}_1 \,.\, \mathrm{D}(m.n) = \mathrm{D}(a,m) = \mathrm{D}(a,n) = 1 \,.\supset.$

·1 $\mathrm{gss}(mn,a) = \mathrm{mlt}[\mathrm{gss}(m,a)\ ,\ \mathrm{gss}(n,a)]$

·2 $\mathrm{gss}(m,a) = \mathrm{mlt}[\mathrm{gss}(x,a) | x, (\mathrm{Np} \upharpoonright \mathrm{N}_1) \frown m/\mathrm{N}_1]$

·3 $\mathrm{gss}(m,a)\ \varepsilon\ \mathrm{N}_1 \frown \Psi m/\mathrm{N}_1$

❋ 38. $p \varepsilon \mathrm{Np}-\iota 2$

·0 $\mathrm{Rpr}p = \mathrm{n} \frown x \ni [\mathrm{gss}(p,x) = p-1]$ Df Rpr

$\mathrm{Rpr}p$ = *radice primitivo de* p, es numero que pertine ad exponente $p-1$, secundum modulo p. Ce denominatione es introducto ab EULERO.

·1 $\mathrm{Num}[1 \cdots (p-1) \frown \mathrm{Rpr}p] = \Phi(p-1)$

EULERO primo demonstra existe radice primitivo de p, sed suo demonstratione habe aliquo mendo (Comm. n. Ac. Petrop. t. 18, p. 85. Primo demonstratione completo pertine ad GAUSS (Disqu. Arith., art. 55).

·2 $\mathrm{Rpr}p = \mathrm{n} \frown x \ni \{ a \ni \mathrm{Np} \frown (p-1)/\mathrm{N}_1 \,.\supset_a.\, x \mid [(p-1)/a] - 1 \varepsilon -\mathrm{n}p \}$

·3 $\mathrm{Rpr}p = \mathrm{n} \frown x \ni [a \varepsilon \mathrm{Np} \frown (p-1)/\mathrm{N}_1 \,.\supset_a.\, -\exists\, y \ni (y^a \,\varepsilon\, x + \mathrm{n}p)]$

·4 $a \varepsilon \mathrm{n}-\mathrm{n}p \,.\, \mathrm{gss}(p,a) < p-1 \,.\, b \varepsilon \mathrm{n} - \mathrm{n}p \frown x \ni [r \varepsilon \mathrm{N}_1 \,.\supset_r.$
$a^r - \varepsilon\, x + \mathrm{n}p \,.\supset:\, m \varepsilon \mathrm{N}_1 \frown \mathrm{gss}(p,a)/\mathrm{N}_1 \,.\, n \varepsilon \mathrm{N}_1 \frown \mathrm{gss}(p,b)/\mathrm{N}_1 \,.$
$\mathrm{D}(m,n) = 1 \,.\, \mathrm{mlt}[\mathrm{gss}(p,a), \mathrm{gss}(p,b)] = mn \,.\supset.$
$\{ a \mid [\mathrm{gss}(p,a)/m] \} \{ b \mid [\mathrm{gss}(p,b)/n] \varepsilon\, \mathrm{n} \frown x \ni [\mathrm{gss}(p,x) > \mathrm{gss}(p.a]$

In generali oporte conatu ut inveni uno radice primitivo de p, et EULERO puta es difficili inveni tali numero (Opusc. Analyt., t. 1, p. 152). In aliquo casu applicatione de P·2·3 es utile.

Ex P·4 GAUSS trahe methodo ut inveni uno radice primitivo de p (Disqu. Arith., n. 73). Circa alio methodo v. OLTRAMARE, J. f. Math. t. 49, a.1855, p. 161; FROLOV, Bull. Soc. math. de France t. 21, a.1893, p. 113; t. 22, a.1894, p. 211.

·5 $p \varepsilon \mathrm{Np}-\iota 3 \,.\supset.\, \Pi[1 \cdots (p-1) \frown \mathrm{Rpr}p] \,\varepsilon\, 1 + \mathrm{N}_0 p$

·6 $p-1 \,\varepsilon\, \mathrm{N}_1 \times (\mathrm{N}_1+1)^2 \,.\supset.\, \Sigma[1 \cdots (p-1) \frown \mathrm{Rpr}p] \,\varepsilon\, \mathrm{n}p$

·7 $p-1 -\varepsilon\, \mathrm{N}_1 \times (\mathrm{N}_1+1)^2 \,.\supset.\, \Sigma[1 \cdots (p-1) \frown \mathrm{Rpr}p] \,\varepsilon$
$(-1) \mid \mathrm{Num}[\mathrm{Np} \frown (p-1)/\mathrm{N}_1] + \mathrm{n}p$

{·5·6·7 GAUSS, Disqu. Arith. art. 80, 81 v. et ARNDT, J. f. Math. t. 31, a.1846, p. 326; HOFMANN, Math. Ann. t, 20, a.1882, p. 471}

❋ 39·0 $a \varepsilon \mathrm{n}-\mathrm{n}p \,.\, u \varepsilon \mathrm{Cls'Np} \,.\supset:$
$a \varepsilon \mathrm{Rpr}u \,.=:\, x \varepsilon u \,.\supset_x.\, a \varepsilon \mathrm{Rpr}x$ Df

·1 $3,5,6,10 \varepsilon$ Rpr{Np⌒[2⌒(2⌒N$_1$)+1]}

·2 2ε Rpr[Np⌒2(Np⌒4N$_0$+1)+1]

·3 -2 ε Rpr[Np⌒2(Np⌒4N$_0$+3)+1]

·4 2 ε Rpr[Np⌒4Np+1]

{·1···4 , v. TCHEBYCHEF, Teoria delle congruenze (trad. MASSARINI) pp. 209-213}

·5 $m\varepsilon$N$_1$+1 .⊃. 3εRpr{Np⌒2^m[Np⌒N$_1$+(9⌒2^{m-2}—1)/2^{m+1}]+1}

{Ce P es in theoria de congruentias de TCHEBYCHEF (trad. MASSARINI, p. 212) sub forma minus utile. In ce forma es in « *Elém. de la th. des nombres, par* E. CAHEN, p. 398}

Existe tabulas de radice primitivo, v.

TCHEBYCHEF, *Teoria delle congruenze* (*trad.* MASSARINI). *Tavola delle radici primitive dei numeri primi da* 3 *a* 353, (pp. 248-287).

WERTHEIM, *Primitive Wurzeln des Primzahlen* 2^nq+1, bei *Welchen* q=1, *oder gleich einer ungeraden Primzahl ist;* Zeitsch. f. Math., t. 25, a.1894, pp. 81-97; — *Tabelle der kleinsten primitiven* W*urzeln* g *aller ungeraden Primzahlen* p *unter* 3000, Acta Math., t. 17, a.1893, pp. 315-320; — *Primitive* W*urzeln der Primzahlen von der Form* $2\pi q^\lambda+1$ *in welcher* q=1 *oder eine ungerade Primzahl ist. Tabelle der kleinsten primitiven* W*urzeln* g *aller Primzahlen* p *zwischen* 3000 *und* 10000, Acta Math., t. 20, a.1896, pp. 143-157; — Berichtigungen zur Tabelle der kleinsten primitiven Wurzeln unter 10000 (Acta Math., t. 22, 1898).

* 40. $p\varepsilon$ Np-ι2 . $a\varepsilon$ Rpr$p$. $b,c\varepsilon$ n-np.⊃:

·0 ^{a}Ind(b,p) = min[N$_0$⌒x∋($a^x\varepsilon$ b+np)]

^{a}Ind(b,p) = indice de b in basi a, secundum modulo p. Ce denominatione et symbolo « Ind » es introducto a GAUSS (Disqu. Arit. art. 57). Theoria de Indice es analogo ad theoria de logarithmo.

·1 ^{a}Ind(b,p) ε 0···$(p-2)$

·2 $k\varepsilon$ n⌒x∋($a^x\varepsilon b$+np) .⊃. $k\varepsilon$ ^{a}Ind(b,p)+n$(p-1)$

·3 ^{a}Ind$(1,p)$=0

·4 ${}^a\mathrm{Ind}(a,p)=1$

·5 $b\varepsilon\, c+\mathrm{n}p \;.\supset.\; {}^a\mathrm{Ind}(b,p)\,\varepsilon\,{}^a\mathrm{Ind}(c,p)+\mathrm{n}(p-1)$

·6 ${}^a\mathrm{Ind}(bc,p)\,\varepsilon\,{}^a\mathrm{Ind}(b,p)+{}^a\mathrm{Ind}(c,p)+\mathrm{n}(p-1)$

·7 $m\varepsilon\mathrm{N}_1 \;.\supset.\; {}^a\mathrm{Ind}(b^m,p)\,\varepsilon\, m\times{}^a\mathrm{Ind}(b,p)+\mathrm{n}(p-1)$

·8 $c\varepsilon\mathrm{Rpr}p \;.\supset.\; {}^c\mathrm{Ind}(b,p)\times{}^a\mathrm{Ind}(c,p)\,\varepsilon\,{}^a\mathrm{Ind}(b,p)+\mathrm{n}(p-1)$

·9 $a\varepsilon\mathrm{Rpr}p \;.\supset:\; c\varepsilon\mathrm{N}_1 \,.\, \mathrm{D}(c,p-1)=1 \;.\supset_c.\; a^c\,\varepsilon\,\mathrm{Rpr}p$

✱ 41. $p\varepsilon\mathrm{Np}-\iota 2 \,.\, a\varepsilon\mathrm{Rpr}p \,.\, b,c\,\varepsilon\,\mathrm{n}-\mathrm{n}p \;.\supset:$

·1 $\mathrm{gss}(p,b) = (p-1)/\mathrm{D}[(p-1),{}^a\mathrm{Ind}(b,p)]$

·2 $n\varepsilon\mathrm{N}_1 \,.\, k\varepsilon\mathrm{n}\cap x\ni(bx^n\varepsilon c+\mathrm{n}p) \;.\supset.$
$n\times{}^a\mathrm{Ind}(k,p)\,\varepsilon\,{}^a\mathrm{Ind}(c,p)-{}^a\mathrm{Ind}(b,p)+\mathrm{n}(p-1)$

In propositione ·2 es uno methodo ut resolve congruentia binomio $bx^n\varepsilon c+\mathrm{n}p$ (v. ARNDT, J. f. math., t. 31, a.1846, p. 333). Ut applica ce methodo oporte tabulas de indice, pro que v. GAUSS, Disqu. Arith., tabula de indice de numero primo ex 3 usque ad 97; — TCHEBYCHEF, Teoria delle congruenze (trad. MASSARINI), v. P 39·4.

✱ 42. $,p\varepsilon\mathrm{Np}-\iota 2 \,.\, m\varepsilon\mathrm{N}_1 \;.\supset.$

·0 $\mathrm{Rpr}p^m = \mathrm{n}\cap x\ni[\mathrm{gss}(p^m,x) = \Phi p^m]$ Df

·1 $m\varepsilon\mathrm{N}_1+1 \;.\supset.\; \mathrm{Rpr}p^m = \mathrm{Rpr}p^2$

·2 $\mathrm{Num}[1\cdots(p^m-1)\cap\mathrm{Rpr}p^m] = \Phi\Phi p^m$

}LEBESGUE, J. de Math., t. 19, a.1854, p. 289, 334{

✱ 43. $m\varepsilon\mathrm{N}_1 \,.\, p\varepsilon\,\mathrm{Np}-\iota 2 \,.\, a\varepsilon\,\mathrm{Rpr}p^m \,.\, b,c\varepsilon\,\mathrm{n}-\mathrm{n}p \;.\supset:$

·0 ${}^a\mathrm{Ind}(b,p) = \min[\mathrm{N}_0\cap x\ni(a^x\varepsilon\, b+\mathrm{n}p^m)]$ Df

·1 ${}^a\mathrm{Ind}(b,p)\,\varepsilon\,0\cdots(\Phi p^m-1)$

·2 $k\varepsilon\,\mathrm{n}\cap x\ni(a^x\,\varepsilon\, b+\mathrm{n}p^m) \;.\supset.\; k\varepsilon{}^a\mathrm{Ind}(b,p^m)+\mathrm{n}\times\Phi p^m$

·3 ${}^a\mathrm{Ind}(1,p^m) =0$

·4 ${}^a\mathrm{Ind}(a,p^m) =1$

·5 $b\varepsilon\, c+\mathrm{n}p^m \;.\supset.\; {}^a\mathrm{Ind}(b,p^m)\,\varepsilon\,{}^a\mathrm{Ind}(c,p^m)+\mathrm{n}\times\Phi p^m$

·6 ${}^a\mathrm{Ind}(bc,p^m)\,\varepsilon\,{}^a\mathrm{Ind}(b,p^m)+{}^a\mathrm{Ind}(c,p^m)+\mathrm{n}\times\Phi p^m$

·7 $n \varepsilon N_1 . \supset . {}^a\mathrm{Ind}(b^n,p^m) \varepsilon n \times {}^a\mathrm{Ind}(b,p) + \mathrm{n} \times \Phi p^m$

·8 $c \varepsilon \mathrm{Rpr} p^n . \supset . {}^c\mathrm{Ind}(b,p^m) \times {}^a\mathrm{Ind}(c,p^m) \varepsilon {}^a\mathrm{Ind}(b,p^m) + \mathrm{n} \times \Phi p^m$

·9 $c \varepsilon N_1 . \mathrm{D}(c, \Phi p^m) = 1 . \supset . a^c \varepsilon \mathrm{Rpr} p^m$

❋ 44. Hp43 $. \supset :$

·1 $\mathrm{gss}(p^m,b) = \Phi p^m / \mathrm{D}[\Phi p^m, {}^a\mathrm{Ind}(b,p^m)]$

·2 $n = \mathrm{mp}[p, b \frown \mathrm{gss}(p,b) - 1] . m \gtreqless n . \supset . {}^a\mathrm{Ind}(b,p^m) \varepsilon N_0 \times p^{n-1}$

·3 ———————————— $. m \leqq n . \supset .$ ——————— $\varepsilon N_0 \times p^{m-1}$

·4 $n \varepsilon N_1 . k \varepsilon \mathrm{n} \frown x \ni (b x^n \varepsilon c + \mathrm{n} p^m) . \supset .$
$n \times {}^a\mathrm{Ind}(k,p^m) \varepsilon {}^a\mathrm{Ind}(c,p^m) - {}^a\mathrm{Ind}(b,p^m) + \mathrm{n} \times \Phi p^m$

❋ 45. $m \varepsilon N_0 . \supset :$

·0 $\mathrm{Rpr} 2^m = \mathrm{n} \frown x \ni [\mathrm{gss}(2^m,x) = \Phi 2^m]$ Df

·1 $\mathrm{Rpr} 1 = \mathrm{n}$

·2 $\mathrm{Rpr} 2 = 2\mathrm{n} + 1$

·3 $\mathrm{Rpr} 4 = 4\mathrm{n} - 1$

·4 $m \varepsilon N_1 + 2 . \supset . - \exists \mathrm{Rpr} 2^m$

·5 $m \varepsilon N_1 . b \varepsilon 2\mathrm{n} + 1 . \supset . \exists (x,y) \ni [x,y \varepsilon N_0 . b \varepsilon (-1)^x 5^y + \mathrm{n} 2^m]$
{GAUSS, Disqu. Arith., art. 91}

❋ 46. $m \varepsilon \iota 0 \cup \iota 1 \cup \iota 2 . a \varepsilon \mathrm{Rpr} 2^m . b \varepsilon 2\mathrm{n} + 1 . \supset .$

·0 ${}^a\mathrm{Ind}(b,2^m) = \min[N_0 \frown x \ni (a^x \varepsilon b + \mathrm{n} 2^m)]$ Df

·1 ${}^a\mathrm{Ind}(b,1) = 0$

·2 $a \varepsilon 2\mathrm{n} + 1 . \supset . {}^a\mathrm{Ind}(b,2) = 1 .$

·3 $a \varepsilon 4\mathrm{n} - 1 . \supset . {}^a\mathrm{Ind}(b,4) \varepsilon \iota 0 \cup \iota 1$

❋ 47·0 $m \varepsilon N_1 . b \varepsilon 2\mathrm{n} + 1 . \supset . \mathrm{Ind}(b,2^m) =$
$\imath (x,y) \ni \{ x \varepsilon \iota 0 \cup \iota 1 . y = \min N_0 \frown y \ni [b \varepsilon (-1)^x 5^y + 2^m \mathrm{n}] \}$ Df

$\mathrm{Ind}(b,2^m)$ es appellato systema de indices de b secundum modulo 2^m. Si es $m \leqq 2$, nos pote semper loque de systema de indices.

N. AMICI in articulo *Risoluzione della congruenza* $x^m \equiv b$ (*mod.* 2^ν),Rend. Circolo Mat. di Palermo, t. 8, a.1894, pp. 187-201,

appella « radice quasi primitivo di 2^ν » numero que pertine ad exponente $2^{\nu-2}$, et supra tali numeros pone fundamento de theoria de indices secundum modulo 2^ν. Ipse ute ce methodo ut resolve congruentia $x^m \varepsilon b + 2^\nu \mathrm{n}$, et $a^x \varepsilon b + 2^\nu \mathrm{n}$, sed me inveni formula de resolutione pro congruentia $x^m \varepsilon b + 2^\nu n$, v. P31·5.

✱ 48. $m \varepsilon \mathrm{N}_1 . \supset .$

·0 $\mathrm{Rpr} m = \mathrm{n} \frown x \ni [\mathrm{gss}(m,x) = \Phi m]$

·1 $\exists \mathrm{Rpr} m .=. m \varepsilon \iota 1 \cup \iota 2 \cup \iota 4 \cup \iota (\mathrm{Np} - \iota 2) \upharpoonright \mathrm{N}_1 \cup \iota 2 (\mathrm{Np} - \iota 2) \upharpoonright \mathrm{N}_1$

{Gauss, Disqu. Arith., art. 92}

Si m non habe radice primitivo, Dirichlet defini systema de indices de m, Berl. Abh, a.1837, p. 45 = Werke, t. 1, p. 313, aut *Vorlesungen*, suppl. 5. — V. et Bennett, London Trans., t. 184, a.1893, p. 189, ubi es et tabulas.

§ 8 Applicationes

✱ 49. $a \varepsilon \mathrm{N}_1 . \supset :$

·1 $\mathrm{n} \frown x \ni (x^{a-1} \varepsilon 1 + \mathrm{n} a) =$
$\mathrm{n} \frown x \ni \{ x \upharpoonright \mathrm{mlt}[\mathrm{D}(a, p-1) | p, \mathrm{Np} \frown a / \mathrm{N}_1] - 1 \varepsilon \mathrm{n} a \}$

·2 $\mathrm{Num}[1 \cdots (a-1) \frown x \ni (x^{a-1} \varepsilon 1 + \mathrm{n} a)] = \Pi [\mathrm{D}(a, p-1) | p, \mathrm{Np} \frown a / \mathrm{N}_1]$

·3 $p, q \varepsilon \mathrm{Np} - \iota 2 . a \varepsilon \mathrm{n}^2 + \mathrm{n} q - \mathrm{n} q . \supset . a \upharpoonright (pq - 1) \varepsilon 1 + pq\mathrm{n}$

·31 $p \varepsilon \mathrm{Np} \frown 4 \mathrm{N}_1 + 3 . 2p - 1 \varepsilon \mathrm{Np} . \supset . 3 \upharpoonright p(2p-1) \varepsilon 1 + \mathrm{N}_1 \times p(2p-1)$

·32 $p \varepsilon \mathrm{Np} \frown 4 \mathrm{N}_1 + 1 . 2p - 1 \varepsilon \mathrm{Np} . \supset . 2 \upharpoonright p(2p-1) \varepsilon 1 + \mathrm{N}_1 \times p(2p-1)$

·33 ———————— . ———————— $. \supset . 3 \upharpoonright p(2p-1) \varepsilon 1 + \mathrm{N}_1 \times p(2p-1)$

·34 $p \varepsilon \mathrm{Np} \frown 20 \mathrm{N}_0 + 1 . 2p - 1 \varepsilon \mathrm{Np} . \supset . 10 \upharpoonright p(2p-1) \varepsilon 1 + \mathrm{N}_1 \times p(2p-1)$

{·1···34 v. meo scripto, *sui numeri composti* etc., Annali di M., s. 3., t. 9, a.1903, pp. 139-160}

✱ 50·1 $p \varepsilon \mathrm{N}_1 . a \varepsilon \mathrm{n} . \mathrm{D}(a,p) = 1 . \mathrm{gss}(p,a) = p - 1 . \supset . p \varepsilon \mathrm{Np}$

{Lucas, *Sur la recherche des grands nombres premiers*, Congrès de Clermont-Ferrand, a.1876}

·2 $q \varepsilon \mathrm{Np} \frown 4 \mathrm{N}_0 + 1 . \supset : 2q + 1 \varepsilon \mathrm{Np} .=. 2^q + 1 \varepsilon \mathrm{N}_1 \times (2q+1)$

·3 $q \varepsilon \mathrm{Np} \cap 4\mathrm{N}_0+3 \,.\supset\!:\, 2q+1 \,\varepsilon\, \mathrm{Np} \,.=.\, 2^q - 1 \,\varepsilon\, \mathrm{N}_1 \times (2q+1)$

{Lucas, Congrès du Havre, 1877}

·4 $q \varepsilon \mathrm{Np} \,.\supset\!:\, 4q+1 \,\varepsilon\, \mathrm{Np} \,.=.$
$2 \uparrow q + 2 \uparrow [(q+1)/2] + 1 \cup 2 \uparrow q - 2 \uparrow [(q+1)/2] + 1 \,\varepsilon\, \mathrm{N}_0 (4q+1)$

·5 $m \varepsilon 2 \uparrow \mathrm{N}_1 \,.\supset\!:\, 2^m+1 \,\varepsilon\, \mathrm{Np} \,.=.\, 3 \uparrow (2^m - 1) + 1 \,\varepsilon\, \mathrm{N}_1 \times (2^m+1)$

{Proth, Corr. N. a. 1878, t. 4, p. 210. Theoremas analogo circa numeros primo de forma 2^m+1 trade Pépin, Compt. R. de l'A. de Paris, 1877, 2° sem., p. 329. Lucas tribue ad se ce P in praefatione de suo *Théorie des Nombres*, sed ibi es errore typographico.

·6 $q \varepsilon \mathrm{Np} \cap 4\mathrm{N}_0+3 \,.\supset\!:\, 6q+1 \,\varepsilon\, \mathrm{Np} \,.=.\, 2 \uparrow 3q + 1 \,\varepsilon\, \mathrm{N}_1 \times (6q+1)$

·7 $q \varepsilon \mathrm{Np} \cap 4\mathrm{N}_1+1 \,.\supset\!:\, 6q+1 \,\varepsilon\, \mathrm{Np} \,.=.\, 2 \uparrow 3q - 1 \,\varepsilon\, \mathrm{N}_1 \times (6q+1)$

·8 $m \varepsilon \mathrm{N}_1+1 \,.\, q \varepsilon \mathrm{Np} \cap [\mathrm{N}_1 + (9 \uparrow 2^{m-2} - 1)/2^{m+1}] \,.\supset\!:$
$2^m q + 1 \,\varepsilon\, \mathrm{Np} \,.=.\, 3 \uparrow 2^{m-1} q + 1 \,\varepsilon\, \mathrm{N}_1 \times (2^m q + 1)$

Vide meo scripto *Delle congruenze binomie* etc., Periodico di Mat., 1903, p. 330.

P·3 es in F1902, §Np7·4, sed non in forma completo.
P·5 = F1902, §Np7·2.